Cisco Unified Communications Manager、リリース 12.5(1)SU6 セキュリティガイド

最終更新：2025 年 12 月 3 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

はじめに xvii

このマニュアルについて xvii

対象読者 xix

ドキュメントの規則 xx

法令遵守 xx

第 I 部：

Unified CM セキュリティの紹介 23

第 1 章

概要 1

システム要件 1

ベストプラクティス 1

デバイスのリセット、サーバとクラスターの再起動、サービスの再起動 2

デバイス、サーバ、クラスター、およびサービスをリセットする 3

バージとのメディア暗号化設定 4

共通アイコン 4

第 2 章

設定 7

セキュリティの構成 7

第 3 章

デフォルトのセキュリティ 11

デフォルトのセキュリティの概要 11

初期信頼リスト 11

ITLRecovery証明書のための証明書管理の変更 13

連携動作と制限事項 13

信頼検証サービス 14
認証、完全性、および認可 14
イメージ認証（Image authentication） 15
デバイス認証 15
ファイル認証 15
シグナリング認証（Signaling Authentication） 16
ダイジェスト認証 16
認証 18
NMAP スキャン操作 19
自動登録 20
Cisco Unified Communications Manager および ITL ファイルを含むクラスタ間で IP 電話を移行する 20
暗号化（Encryption） 21
エンドユーザのログイン資格情報を保護する 22
シグナリングの暗号化 22
メディア暗号化 23
TLS および SIP SRTP の AES 256 暗号化サポート 24
TLS での AES 256 および SHA-2 のサポート 25
SRTP SIP コール シグナリングでの AES 256 サポート 26
Cisco Unified Communications Manager の要件 27
連携動作と制限事項 27
AES 80 ビット認証サポート 27
自己暗号化ドライブ 28
構成ファイルの暗号化 29
デフォルトのセキュリティ管理タスク 29
Cisco Unified IP Phones の ITL ファイルの更新 30
Cisco Unified IP Phone サポートリストの取得 31
クラスタを 8.0 より前のリリースにロールバックする 31
元に戻した後にリリース 8.6 以降に切り替える 32
ITL ファイルの一括リセットの実行 33
CTL ローカルキーのリセット 34

ITLRecovery 証明書の有効期間を表示する 35
認証と暗号化のセットアップ 35

第 II 部： 基本システムセキュリティ 39

第 4 章 証明書 41
証明書の管理 41
証明書の概要 41
証明書の種類 43
電話の証明書タイプ 43
サーバ証明書の種類 44
サードパーティ CA 署名証明書 46
外部 CA からの証明書のサポート 46
証明書署名要求のキー用途拡張 47
証明書のタスク 48
証明書の一括エクスポート 48
証明書の表示 49
証明書のダウンロード 50
中間証明書のインストール 50
信頼証明書の削除 51
証明書署名要求の生成 52
自己署名証明書の生成 55
証明書の再作成 59
信頼ストアへの認証局署名済み CAPF ルート証明書の追加 67
CTL ファイルの更新 67
連携動作と制限事項 67
証明書の監視と失効 68
証明書の監視の概要 68
証明書モニタの設定(Certificate Monitor Configuration) 68
証明書失効の概要 69
証明書失効の設定 69

第 5 章 セキュリティモード 73
セキュリティモードの概要 73
非セキュア モード (デフォルト モード) 73
セキュア モードの設定 73
混合モード 74
セキュリティモードの確認 75
SASTのCTLファイルの役割 76
SIP OAuth モード 77

第 6 章 暗号管理 79
暗号管理 79
推奨される暗号 81
暗号文字列の設定 82
暗号の制限 85
暗号の制限 93

第 7 章 安全なトーンとアイコン 95
セキュアなトーンとアイコンの概要 95
セキュアな電話コールの識別 97
安全なアイコンとトーンのヒント 98
サポート対象デバイスのセキュアトーン 99
保護されたデバイスのセキュアトーン 99
セキュアなアイコンとトーンの設定タスク 100
セキュアアイコンポリシーのセットアップ 100
クラスターの安全通知トーンを有効にする 101
電話機の保護デバイスとしての設定 102
セキュリティ通話とトーンの制限と制約 102

第 8 章 Certificate Authority Proxy 機能 105
認証局プロキシ機能（CAPF）の概要 105

認証局のプロキシ機能の構成タスクフロー 107
サードパーティの認証局のルート証明書のアップロード 109
認証局（CA）ルート証明書のアップロード 109
オンライン認証局の設定 110
オフライン認証局の設定の設定 111
CAPF サービスをアクティブ化または再起動する 112
CAPD 設定をユニバーサル デバイス テンプレートで設定します。 112
バルク Admin による CAPF 設定の更新 114
電話機の CAPF 設定の設定 115
キープアライブ タイマーの設定 116
認証局のプロキシ機能の管理タスクフロー 116
古い LSC レポートの実行 117
CAPF 経由の LSC 生成 117
保留中の CSR リストの表示 118
古い LSC 証明書の削除 118
CAPF システムの相互作用 119
7942 および 7962 電話機を含む CAPF の例 120
IPv6 アドレッシングとの CAPF のインタラクション 121

第 9 章 TFTP 暗号化 123
TFTP 暗号化構成ファイルの概要 123
TFTP 暗号化構成ファイルのヒント 124
電話設定ファイルの暗号化タスク フロー 125
TFTP 暗号化を有効にする 126
SHA-512 署名アルゴリズムの設定 126
LSC または MIC 証明書のインストールを確認する 127
CTL ファイルの更新 128
サービスの再起動 128
電話をリセット 129
TFTP 暗号化構成ファイルを無効にする 129

第 10 章 電話機のセキュリティ 131

電話のセキュリティの概要 131

電話セキュリティ強化の概要 132

電話セキュリティ強化のセットアップ 136

信頼できるデバイス 137

Cisco Unified Communications Manager Administration 138

電話機モデルのサポート 138

電話セキュリティ設定の表示 139

電話セキュリティのセットアップ 139

優先ベンダー SIP 電話セキュリティのセットアップ 140

優先ベンダー SIP 電話セキュリティ プロファイル デバイスごとの証明書のセットアップ 140

優先ベンダー SIP 電話セキュリティ プロファイルの共有証明書のセットアップ 141

あるクラスターから別のクラスターに電話を移行する 142

電話のセキュリティ インタラクションと制限事項 143

電話セキュリティ プロファイル 143

電話セキュリティ プロファイルの設定項目 145

電話セキュリティ設定のタスクフロー 159

電話セキュリティ プロファイルの検索 160

電話セキュリティ プロファイルのセットアップ 161

電話へのセキュリティ プロファイルの適用 161

電話セキュリティ プロファイルを電話と同期する 162

電話セキュリティ プロファイルの削除 163

電話セキュリティ プロファイルで電話を検索する 163

SIP トランク セキュリティ プロファイルの相互作用と制限 164

SIP 電話のダイジェスト認証の概要 165

SIP 電話のダイジェスト認証の前提条件 165

SIP 電話のダイジェスト認証の設定タスク フロー 165

電話ユーザーにダイジェスト信用証明書を指定する 166

電話セキュリティ プロファイルでダイジェスト認証を有効にする 167

電話にダイジェスト認証を指定する 167
SIP ステーションレルムの設定 167
エンドユーザーのダイジェスト認証情報の設定 168

第 11 章 セキュアな電話会議リソースのセットアップ 169
セキュアな会議 169
会議ブリッジの要件 170
セキュア電話会議アイコン 171
セキュア電話会議の状況 172
Ad Hoc 電話会議のリスト 173
最低セキュリティ レベルの Meet-Me 電話会議 174
Cisco Unified IP Phone のセキュアな電話会議とアイコンのサポート 175
セキュアな会議 CTI サポート 176
トランクおよびゲートウェイでのセキュアな電話会議 176
CDR データ 176
連携動作と制限事項 176
Cisco Unified Communications Manager とセキュアな電話会議との相互作用 176
セキュアな電話会議での Cisco Unified Communications Manager の制限 177
電話会議リソースを保護するためのヒント 178
セキュアな電話会議ブリッジのセットアップ 180
Cisco Unified Communications Manager Administration でセキュアな電話会議ブリッジをセットアップする 181
ミートミー電話会議の最低セキュリティレベルのセットアップ 182
セキュアな電話会議用のパケットキャプチャのセットアップ 182

第 12 章 ボイスメッセージ ポートのセキュリティ設定 185
ボイスメッセージのセキュリティ 185
ボイスメッセージのセキュリティ設定のヒント 186
セキュアなボイスメッセージ ポートのセットアップ 187
単一のボイスメッセージ ポートへのセキュリティ プロファイルの適用 188
ボイスメールポートウィザードを使用してセキュリティプロファイルを適用 188

第 13 章 トランクおよびゲートウェイ SIP セキュリティ 191
トランクおよびゲートウェイ SIP セキュリティの概要 191
SIP トランク暗号化 191
Cisco IOS MGCP ゲートウェイ暗号化 192
H.323 ゲートウェイおよび H.323/H.225/H.245 トランク暗号化 193
SIP トランク セキュリティ プロファイルの設定について 195
SIP トランク セキュリティ プロファイルのセットアップのヒント 195
トランクとゲートウェイの SIP セキュリティ タスク フローの設定 196
セキュアなゲートウェイとトランクのセットアップ 196
SIP トランク セキュリティ プロファイルのセットアップ 197
SIP トランク セキュリティ プロファイルの設定項目 198
SIP トランク セキュリティ プロファイルの適用 205
SIP トランクと SIP トランク セキュリティ プロファイルを同期する 206
Unified Communications Manager Administration を使用して SRTP を許可する 207

第 14 章 Cisco CTL クライアントのセットアップ 209
Cisco CTL セットアップについて 209
復旧用 CTL ファイルに 2 番目の Sast ロールを追加 211
CLI による SIP Oauth の構成 212
Cisco CTL Provider Service をアクティベートする 213
Cisco CAPF サービスのアクティベーション 214
セキュアポートのセットアップ 214
Cisco CTL クライアントのセットアップ 216
SASTのCTLファイルの役割 218
あるクラスターから別のクラスターに電話を移行する 218
eToken ベースの CTL ファイルからトークンレス CTL ファイルへの移行 220
CTL ファイルの更新 220
Cisco Unified Communications Manager セキュリティモードの更新 221
Cisco CTL ファイルの詳細 222
Cisco Unified Communications Manager セキュリティモードの確認 223

Smart Card サービスを開始または自動に設定する 224
Cisco CTL クライアントの確認またはアンインストール 225

第 15 章 TLS セットアップ 227
TLS の概要 227
TLS 前提条件 227
TLS 設定タスク フロー 228
最小 TLS バージョンの設定 229
TLS 暗号化の設定 230
SIP トランク セキュリティ プロファイルでの TLS の設定 230
SIP トランクへのセキュア プロファイルの追加 231
電話セキュリティ プロファイルでの TLS の設定 231
セキュアフォンプロファイルを電話に追加する 232
セキュア電話プロファイルをユニバーサル デバイス テンプレートに追加する 233
TLS の連携動作および制限 234
TLS の連携動作 234
TLS の制限 234

第 III 部 : ユーザセキュリティ 241

第 16 章 アイデンティティ管理 243
ユーザセキュリティの概要 243
ID 管理の概要 244
SAML SSO の展開 244
[LDAP認証(LDAP Authentication)] 246
LDAP 認証の設定 246
ローカルデータベース認証 247
Oauth フレームワーク 248
SIP Oauth モードの設定 249
既存の OAuth 更新トークンの取り消し 249

第 17 章 資格情報ポリシー 251
資格情報ポリシーの概要 251
クレデンシャル ポリシーの JTAPI および TAPI のサポート 253
デフォルトのクレデンシャル ポリシーの設定 253
ユーザ資格情報または資格情報ポリシーの編集 254
PIN同期の有効化 255
認証アクティビティのモニタ 257
クレデンシャル キャッシングの設定 258
セッション終了の管理 258

第 18 章 連絡先検索認証。 261
連絡先検索の認証の概要 261
連絡先検索の認証タスクフロー 261
連絡先検索認証のための電話サポートの確認 262
連絡先検索の認証の有効化 262
連絡先検索用のセキュアなディレクトリ サーバの設定 263

第 IV 部 : 高度なシステムセキュリティ 265

第 19 章 FIPS モードのセットアップ 267
FIPS セットアップ 267
FIPS 140-2 モードを有効にする 269
CiscoSSH サポート 271
FIPS 140-2 モードを無効にする 271
FIPS 140-2 モードのステータスの確認 272
FIPS 140-2 モードサーバの再起動 272
FIPS モードの制限 273
強化されたセキュリティ モード 273
セキュリティ強化モードを設定する 275
共通基準モード 276

コモンクライテリア設定タスクフロー 276
[VLANの有効化（Enable TLS）] 277
共通基準モードを設定する 278

第 20 章 共通基準認定ソリューションの ECDSA サポート 281
ECDSA による認定ソリューションの Common Criteria サポート 281
Certificate Manager の ECDSA サポート 281
SIP ECDSA サポート 282
CAPF ECDSA サポート 283
エントロピー 284
HTTPS サポートの設定ダウンロード 284
CTI マネージャサポート 285

第 21 章 V.150 の最小必須要件 287
V.150 の概要 287
V.150 タスク フローを設定する 287
メディア リソース グループのタスク フローを設定する 289
非 V.150 エンドポイントのメディア リソース グループを設定する 290
非 V.150 エンドポイントのメディア リソース グループ リストを設定する 290
V.150 エンドポイントのメディア リソース グループを設定する 291
V.150 エンドポイントのメディア リソース グループ リストを設定する 291
Cisco ゲートウェイ V.150 (MER) を設定する 292
V.150 MGCP ゲートウェイ ポート インターフェイスを設定します 293
V.150 SCCP ゲートウェイ ポート インターフェイスを設定する 293
電話の V.150 サポートを設定する 294
SIP トランクの設定タスク フロー 295
V.150 の SIP プロファイルの設定 296
クラスター全体の V.150 フィルターを設定する 296
V.150 フィルタを SIP トランク セキュリティ プロファイルに追加 297
V.150 の SIP トランクを設定する 297

第 22 章 IPSec のセットアップ 299

IPSec の概要 299

第 23 章 CTI、JTAPI、および TAPI の認証と暗号化のセットアップ 301

CTI、JTAPI、および TAPI アプリケーションの認証 301

CTI、JTAPI、および TAPI アプリケーションの暗号化 303

CTI ポートのより強力な暗号スイート 304

CTI、JTAPI、および TAPI アプリケーションの CAPF 関数 305

CAPF システム インタラクションと CTI、JTAPI、および TAPI アプリケーションの要件 306

認証局プロキシ 機能 サービスのアクティベーション 306

アプリケーションユーザまたはエンドユーザの CAPF プロファイルのセットアップ 307

CAPF の設定項目 308

CAPF サービス パラメータの更新 310

アプリケーション ユーザ CAPF またはエンド ユーザ CAPF プロファイルの削除 311

CTI、JTAPI、および TAPI の保護 312

アプリケーション ユーザとエンド ユーザをセキュリティ関連のアクセス コントロール グループに追加する 314

JTAPI/TAPI セキュリティ関連のサービスパラメータのセットアップ 315

アプリケーションまたはエンドユーザの証明書操作状況を表示する 316

第 24 章 安全な録画とモニタリング 317

セキュアな通話のモニタリングと録音のセットアップについて 317

セキュア通話の監視と録音の設定 318

第 25 章 VPN クライアント 319

VPN クライアントの概要 319

VPN クライアント設定のタスク フロー 319

Cisco IOS の前提条件の完了 321

IP Phone をサポートするための Cisco IOS SSL VPN の設定 321

AnyConnect 用の ASA 前提条件への対応 323
IP Phone での VPN クライアント用の ASA の設定 324
VPN コンセントレータの証明書のアップロード 326
VPN ゲートウェイの設定 327
VPN クライアントの VPN ゲートウェイ フィールド 328
VPN グループの設定 328
VPN クライアントの VPN グループ フィールド 329
VPN プロファイルの設定 329
VPN クライアントの VPN プロファイル フィールド 330
VPN 機能のパラメータの設定 331
VPN 機能のパラメータ 331
共通の電話プロファイルへの VPN の詳細の追加 333

第 26 章 オペレーティング システムとセキュリティ強化 335
セキュリティの強化 335

第 V 部： トラブルシューティング 339

第 27 章 セキュリティのトラブルシューティングの概要 341
Remote Access 341
Cisco Secure Telnet 342
ファイアウォールによる保護 342
Cisco Secure Telnet の設計 342
Cisco Secure Telnet の構造 343
リモート アカウントの設定 343

はじめに

Cisco Unified Communications Manager システムにセキュリティメカニズムを実装することで、電話や Unified Communications Manager サーバーのなりすまし、データの改ざん、コールシグナリング/メディアストリームの改ざんを防止します。

CiscoIP テレフォニーネットワークは、認証された通信ストリームを確立して維持します。ファイルを電話に転送する前にファイルにデジタル署名し、Cisco Unified IP Phone 間のメディアストリームとコールシグナリングを暗号化します。

- このマニュアルについて （xvii ページ）
- 対象読者 （xix ページ）
- ドキュメントの規則 （xx ページ）
- 法令遵守 （xx ページ）

このマニュアルについて

『セキュリティガイド』には以下の部分と簡単な説明があります。

表 *1* : 部分と説明

FCC パート 15.247	説明
CUCM セキュリティの紹介	次のトピックに関するセキュリティの概要についての情報を提供します。 • システム要件 • 共通アイコン • ベストプラクティス また、システムでセキュリティを設定するための概要も提供します。

FCC パート 15.247	説明
基本システムセキュリティ	システムの基本的なセキュリティの設定に関する次の項目に関する情報を提供しています。 • 証明書 • セキュリティモード • 暗号管理 • セキュアなトーンとアイコン • TFTP 暗号化 • 電話機のセキュリティ • トランクおよびゲートウェイ SIP セキュリティ • TLS セットアップ

ユーザセキュリティ	システムのユーザーセキュリティ設定に関する以下のトピックの情報を提供します。
	• アイデンティティ管理
	  • ユーザ アクセス制御
	  • 資格情報ポリシー
	• ディレクトリアクセス
	  • 連絡先検索の認証設定
	  • 連絡先検索用のセキュアなディレクトリ サーバの設定

FCC パート 15.247	説明
アドバンストシステムセキュリティ	システムのユーザーセキュリティ設定に関する以下のトピックの情報を提供します。 • FIPS モード • 強化されたセキュリティ モード • 共通基準モード • Cisco V.150 の最小基本要件 • ECDSA および RSA • IPsec ポリシー • CTI の認証と暗号化のセットアップ • JTAPI、TAPI • 安全な通話の監視と録音 • VPN クライアント
付録	システムをセキュリティ保護するための次の項目に関する情報を提供します。 • 追加のセキュリティ構成 • 用語と頭字語 • 連携動作と制限事項 • ハイパーテキスト転送プロトコル（HTTPS）上のセキュアソケットレイヤー • トラブルシューティング情報 • リモートアカウント • ログの詳細 • 一般的な脆弱性と PSIRT • OS の強化

対象読者

このガイドの対象読者は、以下のとおりです。

• システム管理者

- 電話管理者

Unified Communications Manager の通話セキュリティ機能を設定します。

ドキュメントの規則

このセクションでは、このガイドで従うドキュメントの表記規則について説明します。

メモの表記規則は次のとおりです。

（注） 重要な情報や追加の情報に注目することを読者に示唆します。

ヒントでは、次の表記規則を使用します。

ヒント 次は役に立つヒントです。

警告は、次の表記規則を使用します。

注意 読者は注意が必要であることを意味します。 このような場合にも、指示を注意深く読んでください。そうしないと装置の破損やデータ損失が発生する可能性があります。

警告は、次の表記規則を使用します。

注目 「読者は注意を払うべき」という意味です。 このような場合にもインストール方法の説明をよく読んでください。さもないと装置の破損やデータ損失が発生する可能性があります。

警告

警告 読者 **は必ず** 手順に従う必要があります。 このような場合にも、指示を注意深く読んでください。そうしないと装置の破損やデータ損失が発生する可能性があります。

法令遵守

Unified Communications Manager (セキュリティ) 製品には、暗号機能およびそのインポート/エクスポート情報が含まれています。 情報の転送と使用は、米国および現地の準拠法に従います。 Cisco 暗号化製品の配信は、暗号化をインポート、エクスポート、配布、または使用するサードパーティの権限を意味するものではありません。輸入業者、輸出業者、ディストリビュー

ター、およびユーザは、米国および現地の法律を遵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したものと見なされます。米国および地域の法律に準拠できない場合は、直ちに本製品を返品してください。

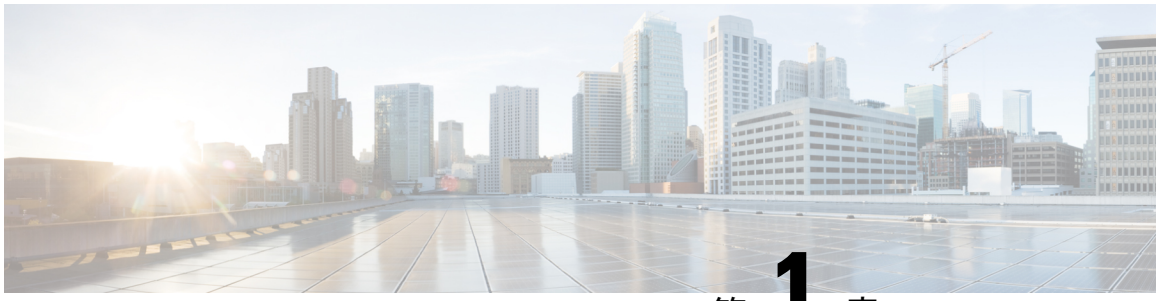
米国輸出規制の詳細については、 http://www.access.gpo.gov/bis/ear/ear_data.htmlを参照してください。

はじめに

第 I 部

Unified CM セキュリティの紹介

- 概要 （1 ページ）
- 設定 （7 ページ）
- デフォルトのセキュリティ （11 ページ）



第 1 章

概要

- システム要件 （1 ページ）
- ベストプラクティス （1 ページ）
- 共通アイコン （4 ページ）

システム要件

Unified Communications Managerを認証または暗号化するためのシステム要件は以下のとおりです。

- Cisco Unified Communications Manager Administration パブリッシャーの Unified Communications Manager CLI にログインし、**util ctl** コマンドを実行して、クラスタを混合モード（セキュアモード）に設定します。
- ローカルで有効な証明書 (LSC) はすべての電話に存在し、 Unified Communications Manager との TLS 接続を認証します。

（注） LSC が存在しない場合、一部のエンドポイントは MIC を使用しますが、LSC を使用することを常に推奨します。

ベストプラクティス

Cisco は以下のベスト プラクティスを強く推奨します。

- 大規模なネットワークに展開する前に、安全なラボ環境でインストールと構成のタスクを必ず実行してください。
- リモートロケーションにあるゲートウェイおよび他のアプリケーションサーバに IPSec を使用してください。

警告 これらのインスタンスで IPSec を使用できないと、セッション暗号化キーがクリアテキストで送信されてしまいます。

- 通話料金の不正を防止するには、 Cisco Unified Communications Manager システム設定ガイドに記載されている会議の強化機能を設定します。 同様に、設定タスクを実行して、通話の外部転送を制限できます。 このタスクの実行方法の詳細は、[Cisco Unified Communications Manager 機能設定ガイド] を参照してください。

デバイスのリセット、サーバとクラスターの再起動、サービスの再起動

リセット、再起動、および再起動の詳細を含むセキュリティアクションを次の表に示します。

表 *2:* リセット、再起動、再起動の詳細を含むセキュリティ アクション:

シリアル番号	操作	リセットする (はい/いいえ)	再起動 (はい/いいえ)
1	セキュリティプロファイルの適用	可	不可
2	電話セキュリティ強化の適用	—	—
3	セキュリティモードの変更	はい。 すべてのデバイス	はい。 CallManager サービスの再起動
4	CTL ファイルの更新	—	はい。暗号化および認証されたすべての電話は、更新された CTL ファイルを取得するためにリセットする必要があります。
5	TLS 接続用のポートの更新	—	はい。 CTL プロバイダーサービスを再起動する。
6	CAPF サービス パラメータの更新/設定	—	はい。 Cisco 認証局プロキシ機能サービスを再起動します

シリアル番号	操作	リセットする (はい/いいえ)	再起動 (はい/いいえ)
7	CTL プロバイダー サービスを開始または停止する	—	はい。 すべての Cisco CallManager および Cisco TFTP サービスを再起動する
7	セキュアな SRST 参照を設定する	はい。 依存デバイスをリセットする	—
8	Smart Card サービスを [開始] および [自動] に変更します。	—	可
9	アプリケーションのユーザ CAPF プロファイルに関連するセキュリティ関連のサービスパラメータを設定します。	—	はい。 Cisco IP Manager Assistant サービス、Cisco Web Dialer Web Service、および Cisco Extended Function サービスを再起動してください後。

Unified Communications Manager サービスを再起動するには『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

電話設定の更新後に 1 台の端末をリセットする方法については、「電話セキュリティプロファイルの適用」に関するトピックを参照してください。

デバイス、サーバ、クラスター、およびサービスをリセットする

このセクションでは、 Cisco Unified Serviceabilityのデバイス、サーバ、クラスタ、サービスをいつリセットするかについての情報を提供します。

クラスター内のすべてのデバイスをリセットするには、以下の手順を実行します。

手順

ステップ 1 Unified Communications Managerから、 **システム** > **CiscoUnifiedCM**を選択します。

ステップ 2 **[検索(Find)]** をクリックします。

設定済み Unified Communications Manager サーバの一覧が表示されます。

ステップ 3 リセットする端末の Unified Communications Manager を選択します。

ステップ 4 [**リセット**（**Reset**）] をクリックします。

ステップ 5 クラスター内の各サーバに対して、手順 2 と手順 4 を実行します。

バージとのメディア暗号化設定

Cisco Unified IP 電話 7962 および 7942 の暗号化用にバージを設定し、Cisco Unified Communications Manager Administration で次のタスクを実行します。

- CTL クライアントの Cluster Security Mode パラメータを更新します。
- 組み込みブリッジ有効パラメータを **[サービスパラメータ（Service Parameter）]** ウィンドウで更新します。

タスクが完了すると、次のメッセージが表示されます。

注目 Cisco Unified IP 電話 モデル 7962 および 7942 で暗号化を設定すると、暗号化された通話に参加している場合、暗号化されたデバイスは割り込み要求を受け入れることができません。 コールが暗号化されている場合、割り込みは失敗します。

暗号化セキュリティプロファイルが設定された Cisco Unified IP 電話 7962 および 7942 では、**[電話機の設定（Phone Configuration）]** ウィンドウにメッセージが表示されません。 [内蔵ブリッジ（Built In Bridge）] 設定で **[デフォルト（Default）]** を選択するか、またはデフォルト設定が [デフォルト（Default）] になっています。 どちらを選択しても同じ制限が適用されます。

ヒント 変更が反映されるように、依存する CiscoIP デバイスをリセットします。

共通アイコン

Unified Communications Manager は、通話に参加しているすべてのサーバとデバイスに設定されたセキュリティ レベルに基づいて、通話のセキュリティ ステータスを提供します。

セキュリティ アイコンをサポートするすべての電話に、コール セキュリティ レベルが表示されます。

- シールド アイコンは、認証されたシグナリング セキュリティレベルの通話に表示されます。 シールドは、Cisco IP デバイス間の安全な接続を識別します。つまり、デバイスは認証されており、暗号化されたシグナリングを使用しています。
- 暗号化されたメディアでの通話にはロック アイコンが表示されます。これは、デバイスが暗号化されたシグナリングと暗号化メディアを使用していることを意味します。

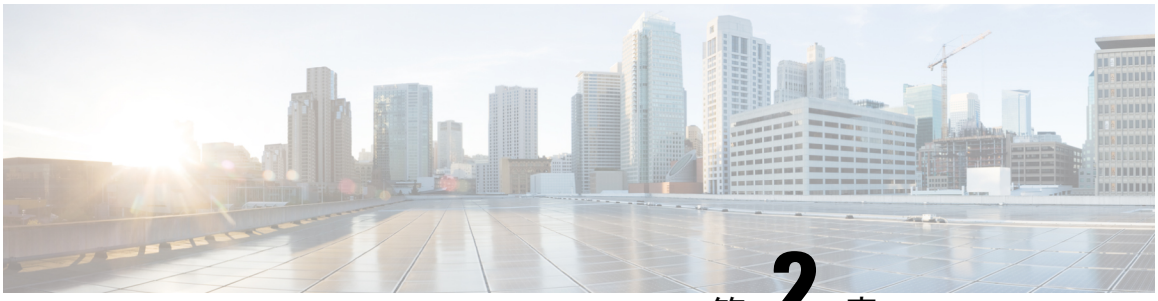
（注） 一部の電話モデルはロック アイコンのみを表示します。 詳細については、使用している Cisco IP Phones のそれぞれのドキュメントを参照してください。

コールのセキュリティ ステータスは、ポイントツーポイント、クラスタ内、クラスタ間、およびマルチホップ コールに対して変更できます。 SCCP 回線、SIP 回線、H.323 シグナリングは、参加エンドポイントへのコール セキュリティ ステータス変更の通知をサポートしています。

音声とビデオのコールは、コール セキュリティ ステータスの基礎を形成します。 通話は、音声とビデオの両方がセキュアである場合にのみセキュアです。

（注） パラメータ値が True で、音声が保護されている場合、「Override BFCP Application Encryption Status when Designating Call Security Status」サービスパラメータはロックアイコンを表示します。 この条件は、他のすべてのメディア チャンネルのセキュリティ ステータスを無視します。 既定のパラメータ値は False です。

電話会議および割り込みコールの場合、セキュリティ アイコン は電話会議のセキュリティ ステータスを表示します。



第 2 章

設定

• セキュリティの構成 （7 ページ）

セキュリティの構成

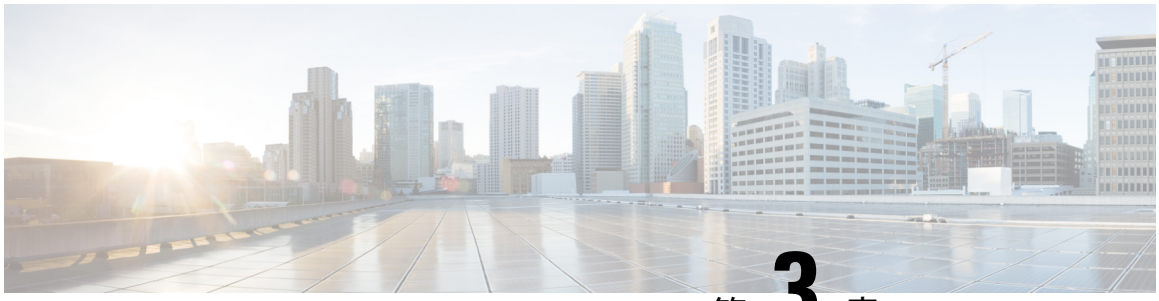
この章では、エンドツーエンドのセキュリティソリューション、さまざまなセキュリティタスクフローのリファレンス、およびその簡単な説明を提供します。

表 *3:* セキュリティの構成

ステップ	手順	説明
ステップ 1	証明書の生成	システムの証明書を構成し、交換します。
ステップ 2	証明書の監視と失効を設定する	証明書の期限切れを監視し、Online Certificate Status Protocol (OCSP) を通じて自動的に証明書を失効させるようにシステムを設定します。
ステップ 3	混合モードを有効にする	混合モードが有効な場合、Cisco Unified IP 電話、TelePresence Endpoints、OAuth なしの Jabber を導入している場合、システムはセキュリティのために Certificate Trust List（CTL）ファイルを使用します。
ステップ 4	認証局プロキシ 機能 (CAPF) を設定する	電話の LSC 証明書を生成するように CAPF を設定します。
ステップ 5	暗号化 TFTP を設定する	暗号化 TFTP を設定して、電話機に送信される初期電話設定ファイルが暗号化されるようにします。
ステップ 6	電話セキュリティを設定する	TFTP 暗号化や電話の TLS シグナリングなどの項目を含むように電話セキュリティ プロファイルを設定します。

ステップ	手順	説明
ステップ 7	電話強化の設定	オプションの製品固有の設定を行い、電話への接続を強化します。
ステップ 8	セキュア トランクの設定	セキュアなトランクを設定して、トランクで TLS とダイジェスト認証を有効にします。
ステップ 9	トランクで SIP を有効にする	SRTP の SIP トランクを設定します。
ステップ 10	SAML SSO の有効化	Identity Management フレームワークを設定します。 Identity Management には SAML SSO を推奨します。 ただし、LDAP 認証またはローカル認証を使用することもできます。
ステップ 11	ユーザ アクセスの設定	エンドユーザーをアクセスコントロールグループに割り当て、彼らが必要とする役割とアクセス権限が含まれています。
ステップ 12	資格情報ポリシーを設定する	ユーザパスワード、ユーザ PIN、およびアプリケーションユーザパスワードのデフォルトのクレデンシャルポリシーを設定します。
ステップ 13	連絡先検索の認証を設定する	会社のディレクトリを保護するために、すべてのディレクトリ検索の認証を確保します。
ステップ 14	[VLANの有効化（Enable TLS）]	電話セキュリティおよびトランク セキュリティ プロファイルを通じて TLS シグナリングを設定します。
ステップ 15	暗号管理の設定	システムでサポートされている暗号化のリストをカスタマイズします。
ステップ 16	IPSec ポリシーを設定する	システムに IPSec ポリシーを設定します。
ステップ 17	ゲートウェイセキュリティの設定	システムのセキュアゲートウェイを設定します。
ステップ 18	OS 強化の設定します。	OS 強化を設定します。
ステップ 19	FIPS の設定	暗号化とデータ セキュリティに関するコンプライアンス ガイドラインを満たすために、FIPS モード、強化されたセキュリティ モード、および共通基準モードを設定します。

ステップ	手順	説明
ステップ 20	セキュリティ機能を設定する	次のようなオプションのセキュリティ機能を設定します。 • セキュアなモニタリングと録画 • 安全な電話会議 • 安全なトーンとアイコン • V.150 • モバイルおよびリモート アクセス • AS-SIP



第 3 章

デフォルトのセキュリティ

- デフォルトのセキュリティの概要 （11 ページ）
- 暗号化（Encryption） （21 ページ）
- デフォルトのセキュリティ管理タスク （29 ページ）

デフォルトのセキュリティの概要

デフォルトのセキュリティ機能は、追加の設定要件を必要とせずに、サポートされている Cisco Unified IP 電話 に対して基本レベルのセキュリティを提供します。

この機能は、サポートされている IP 電話に次のデフォルト セキュリティを提供します。

- TFTP のデフォルト認証
- オプションの暗号化
- 証明書の検証

デフォルトのセキュリティは以下のコンポーネントを使用して、安全ではない環境で基本的なセキュリティを提供します。

- Identity Trust List（ITL）：このファイルは TFTP サービスがクラスタのインストール時に有効化された後にのみ作成され、信頼を確立するために Cisco Unified IP 電話 により使用されます。
- 信頼検証サービス：このサービスはすべての Unified Communications Manager ノードで実行され、Cisco Unified IP 電話 の証明書の認証を行います。 TVS 証明書は他のいくつかの重要な証明書と共に ITL ファイルにバンドルされています。

初期信頼リスト

初期セキュリティには初期信頼リスト（ITL）ファイルが使用され、エンドポイントが Unified Communications Manager を信頼できるようになります。 ITL では、セキュリティ機能を明示的に有効にする必要はありません。 TFTP サービスが有効になり、クラスターがインストールさ

れると、ITL ファイルが自動的に作成されます。 Unified Communications Managerの TFTP サーバの秘密鍵は ITL ファイルへの署名に使用されます。

Unified Communications Manager クラスタまたはサーバがノンセキュアモードの場合、ITL ファイルはサポートされている Cisco Unified IP 電話毎にダウンロードされます。 CLI コマンド **admin:show itl**を使用して、ITL ファイルのコンテンツを表示できます。

Cisco Unified IP 電話 は、次のタスクを実行するために ITL ファイルを必要とします。

- CAPF との安全な通信、これは設定ファイルの暗号化をサポートするための前提条件です。
- 構成ファイルの署名を認証する
- TVS を使用して HTTPS を確立する際に、EM サービス、ディレクトリ、MIDlet などのアプリケーションサーバを認証します。

Cisco IP 電話に既存の CTL ファイルがない場合、最初の ITL ファイルが自動的に信頼されます。 TVS は署名者に対応する証明書を返すことができなければなりません。

Cisco IP 電話に既存の CTL ファイルがある場合、その CTL ファイルを使用して ITL ファイルの署名を認証します。

（注） SHA-1 または MD5 アルゴリズムの値は、Initial Trust List (ITL) ファイルの値が変更された場合にのみ変更されます。 ITL ファイルのチェックサム値を使用して、Cisco IP 電話の ITL ファイルと Unified Communications Manager クラスタ間の違いを識別することができます。 ITL ファイルのチェックサム値は、ITL ファイルを変更した場合にのみ変更されます。

初期信頼リスト (ITL) ファイルの形式は CTL ファイルと同じです。 しかし、それはより小さく、無駄のないバージョンです。

次の属性が ITL ファイルに適用されます。

- TFTP サービスがアクティブで、クラスタをインストールすると、システムは ITL ファイルを自動的に構築します。 コンテンツが変更されると、ITL ファイルは自動的に更新されます。
- ITL ファイルは eToken を必要としません。 ソフト eToken (TFTP サーバの CallManager 証明書に関連する秘密鍵) を使用します。
- Cisco Unified IP 電話 は、リセット中、再起動中、または CTL ファイルのダウンロード後に、ITL ファイルをダウンロードします。

ITL ファイルには次の証明書が含まれます:

- ITLRecovery 証明書 - この証明書は ITL ファイルに署名します。
- TFTP サーバの CallManager 証明書—この証明書により、ITL ファイルの署名および電話構成ファイルの署名を認証することができます。
- クラスターで使用可能なすべての TVS 証明書 - これらの証明書により、電話は TVS と安全に通信し、証明書による認証を要求できます。

- CAPF 証明書：この証明書は設定ファイルの暗号化をサポートします。 CAPF 証明書は ITL ファイルで必要ではありませんが (TVS はそれを認証できます)、CAPF への接続を簡素化します。

ITL ファイルには各証明書のレコードが含まれています。各レコードには以下の内容が含まれています。

- 証明書
- Cisco IP 電話で簡単に検索できる事前抽出証明書フィールド
- 証明書の役割（TFTP、CUCM、TFTP+CCM、CAPF、TVS、SAST）

TFTP サーバの CallManager 証明書は、2 つの異なるロールを持つ 2 つの ITL レコードに存在します。

- TFTP または TFTP と CCM ロール：設定ファイルの署名を認証します。
- SAST ロール：ITL ファイルの署名を認証します。

ITLRecovery証明書のための証明書管理の変更

- ITLRecovery の有効期間が 5 年から 20 年に延長され、ITLRecovery 証明書がより長期間同じ状態を維持できるようになりました。

（注） Unified Communications Manager をアップグレードした場合、ITLRecovery 証明書の有効期間は 5 年間のままです。 Unified Communications Manager をアップグレードしている間、証明書は新しいリリースにコピーされます。 しかし、ITLRecovery 証明書を再生成するか、 Unified Communications Manager を新規にインストールすると、ITLRecovery の有効期間が 20 年に延長されます。

- ITLRecovery 証明書を再生成する前に、CLI と GUI の両方に警告メッセージが表示されます。 この警告メッセージは、トークンなしの CTL を使用する場合、および CallManager 証明書を再生成する場合は、CTL ファイルに更新された CallManager 証明書が含まれていること、およびその証明書がエンドポイントに更新されていることを確認するために表示されます。

連携動作と制限事項

ある Unified Communications Manager クラスタに 39 個を超える証明書がある場合、Cisco IP 電話上の ITL ファイルサイズは 64KB を超えます。 ITL ファイルサイズの増加は、電話での ITL の適切な読み込みに影響を与え、その結果、Unified Communications Manager に登録する際に電話の登録が失敗することがあります。

信頼検証サービス

ネットワークには多数の電話が接続されており、これらの電話のメモリ容量は限られています。 Cisco Unified IP 電話 このため、 Unified Communications Manager はTVSを通じてリモートの信頼ストアとして機能し、証明書の信頼ストアを各電話に配置する必要がなくなります。 Cisco Unified IP 電話（電話）は CTL または ITL ファイルを通じて署名または証明書を確認できないため、確認のために TVS サーバと通信します。 このように、すべての Cisco Unified IP 電話（電話）にトラストストアがあるよりも、中央のトラストストアにある方が管理が容易です。

TVS により、HTTPS を確立する際に、EM サービス、ディレクトリ、MIDlet などのアプリケーションサーバを Cisco Unified IP 電話 （電話）で認証できるようになります。

TVS は以下の機能を提供します。

- スケーラビリティ - Cisco Unified IP 電話 （電話）のリソースは信頼する証明書の数に影響されません。
- 柔軟性—信頼できる証明書の追加または削除は、システムに自動的に反映されます。
- デフォルトでのセキュリティ - 非メディアおよびシグナリング セキュリティ機能は既定のインストールに含まれており、ユーザの介入を必要としません。

（注） セキュアなシグナリングとメディアを有効にする場合、CTL ファイルを作成し、クラスタを混合モードに設定します。 CTL ファイルを作成し、クラスタを混合モードに設定するには、CLI コマンド **utils ctl set-cluster 混合モード**を使用します。

以下は、TVS を説明する基本概念です。

- TVS は Unified Communications Manager サーバ上で動作し、Cisco IP Phoneの代わりに証明書の認証を行います。
- Cisco Unified IP 電話 すべての信頼できる証明書をダウンロードする代わりに、TVS のみを信頼する必要があります。
- ITL ファイルはユーザの介入なしで自動的に生成されます。 ITL ファイルは Cisco Unified IP 電話 によりダウンロードされ、そこから信頼が流れます。

認証、完全性、および認可

整合性と認証により、次の脅威から保護します。

- TFTP ファイル改ざん (整合性)
- Unified Communications Manager と電話間のコール処理シグナリングの変更 (認証)
- 中間者攻撃 (認証) です。 頭字語 セクションに定義されています。

- 電話およびサーバでのなりすまし (認証)
- リプレイ攻撃 (ダイジェスト認証)

承認では、認証されたユーザ、サービス、またはアプリケーションが実行できることを指定します。 単一のセッションで複数の認証および認可方法を実装できます。

イメージ認証（Image authentication）

このプロセスにより、IP電話にロードする前に、ファームウェア ロードであるバイナリ イメージの改ざんが防止されます。イメージが改ざんされると、電話機は認証プロセスに失敗し、新しいイメージを拒否します。 画像認証は、Unified Communications Manager のインストール時に自動的にインストールされる、署名されたバイナリファイルを通じて行われます。 同様に、ウェブからダウンロードしたファームウェア更新も署名済みバイナリイメージを提供します。

デバイス認証

このプロセスにより、通信デバイスの ID を検証し、エンティティが要求されているとおりのものであることを確認します。

Unified Communications Manager サーバーとサポートされている Cisco Unified IP Phone 、SIP トランク、または JTAPI/TAPI/CTI アプリケーションの間で端末認証が行われる（サポートされている場合）。認証された接続は、各エンティティが他のエンティティの証明書を受け入れる場合にのみ、これらのエンティティ間で発生します。 相互認証は、この相互証明書交換のプロセスを説明します。

端末認証は、CiscoCTL ファイル（Unified Communications Manager サーバーノードとアプリケーションの認証用）と証明書機関プロキシ機能（端末と JTAPI/TAPI/CTI アプリケーションの認証用）の作成に依存しています。

ヒント SIP トランク経由で接続する SIP ユーザーエージェントは、CallManager 信頼ストアに SIP ユーザーエージェント証明書が含まれており、SIP ユーザーエージェントが Unified Communications Manager 証明書を信頼ストアに含んでいる場合、Unified Communications Manager で認証します。 CallManager トラストストアの更新についての詳細は、この *Unified Communications Manager* リリースをサポートする『Cisco Unified Communications オペレーティングシステム管理ガイド』を参照してください。

ファイル認証

このプロセスでは、電話がダウンロードしたデジタル署名されたファイルを検証します。たとえば、設定、着信音リスト、ロケール、および CTL ファイルです。 電話機は、ファイル作成後にファイルの改ざんが行われていないことを確認するために、署名を検証します。 対応端末については、 「対応電話モデル」をご覧ください。

混合モードでクラスターを設定する場合、TFTP サーバは、着信音リスト、ローカライズ、default.cnf.xml、着信音リスト wav ファイルなどの静的ファイルに.sgn 形式で署名します。 TFTP

サーバは、ファイルにデータ変更があったことを確認するたびに、<device name>.cnf.xml 形式のファイルに署名します。

キャッシュが無効になっている場合、TFTP サーバは署名済みファイルをディスクに書き込みます。 TFTP サーバは保存されたファイルが変更されたことを確認すると、ファイルに再署名します。ディスク上の新しいファイルは、保存されたファイルを削除されると上書きします。電話が新しいファイルをダウンロードする前に、管理者は影響を受けるデバイスを Unified Communications Manager で再起動する必要があります。

TFTP サーバからファイルを受信した後、電話機はファイルの署名を検証することにより、ファイルの整合性を確認します。 電話が認証された接続を確立するには、次の条件が満たされている必要があります。

- 証明書が電話に存在している必要があります。
- CTL ファイルが電話機上に存在している必要があり、さらに Unified Communications Manager のエントリと証明書が CTL ファイル中に存在している必要があります。
- デバイスの認証または暗号化を構成しました。

シグナリング認証（Signaling Authentication）

シグナリング整合性とも呼ばれるこのプロセスは、TLS プロトコルを使用して、送信中にシグナリング パケットに改ざんが発生していないことを検証します。

シグナリング認証は、証明書信頼リスト (CTL) ファイルの作成に依存しています。

ダイジェスト認証

SIP トランクと電話に対するこのプロセスにより、Unified Communications Manager は、Unified Communications Manager に接続するデバイスの身元を問い詰めることができます。 要求されると、デバイスは確認のため、ユーザ名とパスワードのようなダイジェスト資格情報を Unified Communications Manager に提示します。 提示された資格情報がその端末のデータベースで構成されているものと一致する場合、ダイジェスト認証が成功し、Unified Communications Manager が SIP リクエストを処理します。

（注） クラスタ セキュリティ モードはダイジェスト認証には影響しないことに注意してください。

（注） デバイスのダイジェスト認証を有効にすると、デバイスを登録するための一意のダイジェストユーザ ID とパスワードが要求されます。

Unified Communications Manager データベース内の電話ユーザーまたはアプリケーションユーザー用に SIP ダイジェスト認証情報を設定します。

- アプリケーションの場合は、[アプリケーションユーザーの設定（Application User Configuration）] ウィンドウでダイジェスト認証情報を指定します。

- SIP を実行している電話の場合、[エンドユーザ] ウィンドウでダイジェスト認証資格情報を指定します。 ユーザを設定した後で電話に資格情報を関連付けるには、[電話の設定] ウィンドウで [ダイジェスト ユーザ] とエンド ユーザを選択します。 電話をリセットすると、TFTP サーバーが電話に提供する電話設定ファイルに認証情報が含まれるようになります。 TFTP ダウンロードでダイジェスト認証情報が平文で送信されないようにするには、暗号化された電話設定ファイルのセットアップに関するトピックを参照してください。
- SIP トランクで受信したチャレンジについては、領域ユーザー名（デバイスまたはアプリケーションユーザー）とダイジェスト認証情報を指定する SIP 領域を設定します。

SIP を実行している外部電話またはトランクのダイジェスト認証を有効にし、ダイジェスト認証情報を設定すると、Unified Communications Manager は、ユーザー名、パスワード、および領域のハッシュ値を含む認証情報のチェックサムを計算します。 システムは MD5 ハッシュを計算するために、乱数であるナンス値を使用します。 Unified Communications Manager は値を暗号化し、ユーザ名とチェックサムをデータベースに保存します。

チャレンジを開始するために、Unified Communications Manager は SIP 401（未承認）メッセージを使用します。このメッセージには、ヘッダーにナンスとレルムが含まれます。電話またはトランクの SIP デバイス セキュリティ プロファイルで、ナンスの有効時間を設定します。 ナンスの有効時間は、ナンスの値が有効である時間を分単位で指定します。 この時間間隔が終了すると、 Unified Communications Manager は外部デバイスを拒否し、新しい番号を生成します。

（注） Unified Communications Manager は、回線側の電話またはデバイスから発信された SIP 通話のユーザーエージェントサーバー（UAS）、SIPトランクへの発信コールのユーザーエージェント クライアント（UAC）、または回線間またはトランク間接続のバックツーバック ユーザー エージェント（B2BUA）として機能します。 ほとんどの環境で、 Unified Communications Manager は主に SCCP と SIP エンドポイントを接続する B2BUA として機能します。 (SIP ユーザ エージェントは SIP メッセージを発信するデバイスまたはアプリケーションを表します。)

ヒント ダイジェスト認証は完全性や機密性を提供しません。 デバイスの整合性と機密性を確保するには、デバイスが TLS をサポートしている場合、デバイスの TLS プロトコルを構成します。 デバイスが暗号化をサポートしている場合、デバイス セキュリティ モードを暗号化として構成します。 デバイスが暗号化された電話構成ファイルをサポートしている場合、ファイルの暗号化を構成します。

電話のダイジェスト認証

電話のダイジェスト認証を有効にすると、Unified Communications Manager は、キープアライブメッセージを除く、SIP を実行している電話に対するすべての要求に認証を要求します。 Unified Communications Manager は、回線側の電話からのチャレンジには応答しません。

レスポンスを受信した後、Unified Communications Manager はデータベースに保存されているユーザー名のチェックサムを、レスポンスヘッダーの資格情報と照合します。

SIP を実行する電話機は、Unified Communications Manager 領域にあります。これは、Unified Communications Manager Administration のインストール時に定義されます。 SIP ステーション領域のサービス パラメータを使用して、電話に対するチャレンジのための SIP 領域を設定します。 各ダイジェストユーザーは、領域ごとに 1 セットのダイジェスト資格情報を持つことができます。

ヒント エンド ユーザのダイジェスト認証を有効にしているが、ダイジェスト クレデンシャルを設定していない場合、電話は登録に失敗します。 クラスタモードがノンセキュアで、ダイジェスト認証を有効にしてダイジェストクレデンシャルを設定している場合、ダイジェストクレデンシャルが電話に送信され、 Unified Communications Manager は引き続きチャレンジを開始します。

トランクのダイジェスト認証

トランクのダイジェスト認証を有効にすると、Unified Communications Manager は、SIP トランク経由で接続する SIP デバイスおよびアプリケーションからの SIP トランクリクエストをチャレンジします。 システムは、チャレンジ メッセージで Cluster ID エンタープライズパラメータを使用します。 SIP トランクを通じて接続する SIP ユーザーエージェントは、 Unified Communications Manager でデバイスまたはアプリケーションに対して設定した固有のダイジェスト認証情報で応答します。

Unified Communications Manager が SIP トランクリクエストを開始すると、SIP トランクを通して接続する SIP ユーザーエージェントは、 Unified Communications Manager のアイデンティティをチャレンジすることができます。 これらの着信チャレンジの場合、ユーザに要求された資格情報を提供するように SIP レルムを構成します。 Unified Communications Manager が SIP 401（未承認）または SIP 407（プロキシ認証が必要）メッセージを受信すると、 Unified Communications Manager は、トランク経由で接続する領域の暗号化パスワードと、チャレンジ メッセージで指定されているユーザー名を検索します。 Unified Communications Manager はパスワードを解読し、ダイジェストを計算してレスポンスメッセージで提示します。

ヒント 領域は xyz.com などの SIP トランクを介して接続するドメインを表し、リクエストの送信元を特定するのに役立ちます。

SIP 領域を設定するには、SIP トランクのダイジェスト認証に関するトピックを参照してください。 Unified Communications Manager でチャレンジする Unified Communications Manager のユーザーエージェントごとに、SIP 領域、ユーザー名とパスワードを設定する必要があります。 各トユーザーエージェントは、領域ごとに 1 セットのダイジェスト資格情報を持つことができます。

認証

Unified Communications Manager は、認可プロセスを使用して、SIP を実行している電話、SIP トランク、SIP トランク上の SIP アプリケーション要求からの特定のカテゴリのメッセージを制限します。

- SIP INVITE メッセージ、ダイアログ内メッセージ、および SIP を実行している電話の場合、Unified Communications Manager は、コーリングサーチスペースとパーティションを使用した認可を行います。
- 電話からの SIP SUBSCRIBE 要求の場合、Unified Communications Manager は、ユーザーがプレゼンスグループにアクセスするための認証を提供します。
- SIP トランク Unified Communications Manager は、プレゼンスサブスクリプションと特定の非 INVITE SIP メッセージの認証を行います。例えば、ダイヤル外の REFER、一方的な通知、replaces ヘッダーを持つ SIP 要求などです。 ウィンドウで許可された SIP リクエストにチェックを入れて、[SIP トランクセキュリティプロファイルの設定（SIP Trunk Security Profile Configuration）] ウィンドウでの権限を指定します。

SIP トランクアプリケーションの認証を有効にするには、[SIP トランクセキュリティプロファイル] ウィンドウで [アプリケーションレベル認証を有効にする] と [ダイジェスト認証] チェックボックスを選択します。次に、[アプリケーションユーザの構成] ウィンドウで、許可された SIP 要求のチェックボックスをオンにします。

SIP トランク認証とアプリケーションレベル認証の両方を有効にした場合、認証はまず SIP トランクに対して行われ、次に SIP アプリケーションユーザに対して行われます。 トランク Unified Communications Manager はトランクのアクセスコントロールリスト（ACL）情報をダウンロードしてキャッシュします。 ACL 情報が着信 SIP リクエストに適用されます。 ACL が SIP 要求を許可しない場合、通話は 403 Forbidden メッセージで失敗します。

ACL で SIP リクエストが許可されている場合、Unified Communications Manager は SIP トランクセキュリティプロファイルでダイジェスト認証が有効になっているかどうかを確認します。ダイジェスト認証およびアプリケーションレベル認証が有効ではない場合、Unified Communications Manager がリクエストを処理します。 ダイジェスト認証が有効な場合、Unified Communications Manager は受信リクエストに認証ヘッダーが存在することを確認し、ダイジェスト認証を使用してソースアプリケーションを識別します。 ヘッダーが存在しない場合、Unified Communications Manager は 401 メッセージでデバイスにチャレンジを行います。

アプリケーションレベルの ACL が適用される前に、Unified Communications Manager はダイジェスト認証で SIP トランク ユーザー エージェントを認証します。 そのため、アプリケーションレベルの承認を行う前に、SIP トランクセキュリティプロファイルでダイジェスト認証を有効にしておく必要があります。

NMAP スキャン操作

脆弱性スキャンを実行するために、Windows または Linux プラットフォームでネットワークマッパー (NMAP) スキャンプログラムを実行できます。 NMAP は、ネットワーク探索またはセキュリティ監査のための無料のオープン ソース ユーティリティです。

（注） NMAP DP スキャンは、完了までに最大 18 時間かかる場合があります。

構文

nmap-n-vv-sU-p<*port_range*><*ccm_ip_address*>

引数の説明

-n: DNS 解決を行いません。 見つけたアクティブな IP アドレスで逆 DNS 解決を行わないように NMAP に指示します。 DNS は NMAP ビルトイン並列スタブリソルバーを使用しても遅い場合があるため、このオプションによりスキャン時間を大幅に短縮できます。

-v: 冗長レベルを上げます。これにより NMAP は進行中のスキャンに関する詳細情報を出力します。 システムは、開いているポートが見つかると表示し、スキャンに数分以上かかると NMAP が予測した場合は、完了時間の予測を提供します。 このオプションを 2 回以上使用すると、冗長性がさらに高まります。

-sU: UDP ポートスキャンを指定します。

-p: スキャンするポートを指定し、デフォルトを上書きします。 個別のポート番号や、ハイフンで区切られた範囲のポート番号(たとえば、1-1023)も使用可能であることに注意してください。

ccm_ip_address：Cisco Unified Communications Manager の IP アドレス

自動登録

システムは、混在モードとノンセキュアモードの両方で自動登録をサポートしています。既定の構成ファイルも署名されます。デフォルトでのセキュリティをサポートしない Cisco IP 電話には、署名されていないデフォルトの構成ファイルが提供されます。

Cisco Unified Communications Manager および ITL ファイルを含むクラスタ間で IP 電話を移行する

Unified Communications Manager 8.0(1) 以降では、新しいデフォルトによるセキュリティと初期信頼リスト (ITL) ファイルの使用が導入されています。 この新機能により、異なる Unified CM クラスタ間で電話を移動する場合は注意が必要です。また、適切な移行手順に従うようにしてください。

⚠

注意 適切な手順に従わなかった場合、何千という電話の ITL ファイルを手動で削除する必要があります。

新しい ITL ファイルをサポートする Cisco IP 電話は、 Unified CM TFTP サーバからこの特別なファイルをダウンロードする必要があります。 ITL ファイルが電話機にインストールされると、以降のすべての構成ファイルと ITL ファイルの更新は、次のいずれかによって署名されなければなりません。

- 現在電話機にインストールされている TFTP サーバ証明書、または

- クラスターの一つのTVSサービスで検証できるTFTP証明書。 ITL ファイルにリストされているクラスタ内の TVS サービスの証明書を見つけることができます。

この新しいセキュリティ機能を考慮して、電話を 1 つのクラスタから別のクラスタに移動するときに、3 つの問題が発生する可能性があります。

1. 新しいクラスタの ITL ファイルは現在の ITL ファイルの署名者によって署名されていないため、電話は新しい ITL ファイルまたは設定ファイルを受け入れることができません。
2. 電話の既存の ITL にリストされている TVS サーバは、電話が新しいクラスタに移動されると到達できない場合があります。
3. 証明書の検証のために TVS サーバに到達できても、古いクラスタサーバは新しいサーバ証明書を持っていない場合があります。

これら 3 つの問題のうち 1 つ以上が発生した場合、クラスタ間で移動中のすべての電話機から ITL ファイルを手動で削除することが考えられます。 しかし、これは電話の数が増えるにつれて膨大な労力を必要とするため、望ましいソリューションとは言えません。

最も望ましいオプションは、Cisco Unified CM のエンタープライズパラメータ Prepare Cluster for Rollback to pre-8.0. を利用することです。 このパラメータが True に設定されると、電話は空の TVS および TFTP 証明書セクションを含む特別な ITL ファイルをダウンロードします。

電話に空の ITL ファイルがある場合、電話は署名されていない構成ファイルを受け入れ (Unified CM 8.x 以前のクラスタへの移行用)、新しい ITL ファイルを受け入れます (別の Unified CM 8.x クラスタへの移行用)。

空の ITL ファイルは、電話で [**設定** > **セキュリティ** > **信頼リスト** > **ITL**] をチェックすることで確認できます。 古い TVS および TFTP サーバがあった場所に空のエントリが表示されます。

電話は、新しい空の ITL ファイルをダウンロードするためだけに、古い Unified CM サーバにアクセスする必要があります。

古いクラスタをオンラインのままにしておく場合は、[Prepare Cluster for Rollback to pre-8.0 Enterprise パラメーター] を無効にして、デフォルトでのセキュリティを復元してください。

暗号化（Encryption）

ヒント 暗号化機能は、Unified Communications Manager をサーバーにインストールするときに自動的にインストールされます。

この項では、Unified Communications Manager がサポートする暗号化の種類について説明します。

エンドユーザのログイン資格情報を保護する

Unified Communications Manager リリース 12.5 (1) から、すべてのエンドユーザのログイン資格情報が SHA2 でハッシュされ、セキュリティが強化されます。 Unified Communications Manager リリース 12.5 (1) より前では、すべてのエンドユーザのログイン資格情報は SHA1 のみでハッシュされていました。 Unified Communications Manager リリース 12.5 (1) には、[「時代遅れの資格情報アルゴリズムを使用する 」 UCM ユーザ] レポートも含まれています。 このレポートは Cisco Unified Reporting ページから入手できます。 このレポートは、管理者がパスワードまたは PIN が SHA1 でハッシュされたすべてのエンドユーザを一覧表示するのに役立ちます。

SHA1 でハッシュされたすべてのエンドユーザのパスワードまたは PIN は、最初のログインに成功したときに自動的に SHA2 に移行されます。 SHA1 ハッシュされた (期限切れの) 資格情報を持つエンドユーザは、次のいずれかの方法を使用して PIN またはパスワードを更新できます。

- 電話でエクステンション モビリティまたはディレクトリ アクセスにログインして PIN を更新します。
- Cisco Jabber、Cisco Unified Communications セルフケアポータル、または Cisco Unified CM Administration にログインしてパスワードを更新します。

レポートの作成方法の詳細については、*Cisco Unified CM Administration* オンラインヘルプを参照してください。

シグナリングの暗号化

シグナリングの暗号化により、端末との間で Unified Communications Manager サーバ間で送信されるすべての SIP および SCCP シグナリングメッセージが暗号化されます。

シグナリングの暗号化により、当事者、当事者が入力する DTMF 番号、コール ステータス、メディア暗号化キーなどに関連する情報が、意図しないまたは不正なアクセスから確実に保護されます。

混合モードでクラスタを構成する場合、Cisco は Unified Communications Manager でのネットワークアドレス変換 (NAT) をサポートしません。NAT はシグナリング暗号化では機能しません。

ファイアウォールでUDP ALGを有効にして、メディアストリームファイアウォールトラバーサルを許可することができます。 UDP ALG を有効にすると、ファイアウォールの信頼された側のメディアソースは、ファイアウォールを通してメディアパケットを送信することにより、ファイアウォールを通して双方向のメディアフローを開くことができます。

ヒント ハードウェア DSP リソースはこのタイプの接続を開始することができないため、ファイアウォールの外側に存在している必要があります。

シグナリング暗号化は NAT トラバーサルをサポートしていません。 NAT を使用する代わりに、LAN 拡張 VPN の使用を検討してください。

メディア暗号化

Secure Real-Time Protocol (SRTP) を使用するメディア暗号化により、意図した受信者だけが、サポートされているデバイス間のメディアストリームを解釈できるようになります。メディア暗号化には、デバイスのメディア マスター キー ペアの作成、デバイスへのキーの配信、およびキーの転送中の配信のセキュリティ保護が含まれます。 Unified Communications Manager は、主に IOS ゲートウェイと Unified Communications Manager のゲートキーパー制御および非ゲートキーパー制御の H.323 トランク、そして SIP トランクに対して SRTP をサポートしています。

（注） Cisco Unified Communications Manager は、異なるデバイスやプロトコルに対して、異なる方法でメディア暗号化キーを扱います。 SCCP を実行しているすべての電話は、 Unified Communications Manager からメディア暗号化キーを取得します。これにより、TLS 暗号化シグナリングチャネルを使用して、電話へのメディア暗号化キーのダウンロードが保護されます。 SIP を実行している電話は、独自のメディア暗号化キーを生成して保存します。 Unified Communications Manager システムにより生成されるメディア暗号化キーは、H.323 および MGCP の場合は IPSec 保護リンクを介して、また SCCP および SIP の場合は暗号化された TLS リンクを介してゲートウェイに安全に送信されます。

デバイスは、SRTP を使用できるかどうかをネゴシエーションで記述する必要があります。 デバイスが同じコール内の異なるデバイスとのキャッシュされた以前のネゴシエーション SDP を使用する場合、CUCM は SRTP をサポートしません。

デバイスが SRTP をサポートしている場合、システムは SRTP 接続を使用します。 1 つ以上のデバイスが SRTP をサポートしていない場合、システムは RTP 接続を使用します。 SRTP から RTP へのフォールバックは、セキュアなデバイスから非セキュアなデバイスへの転送、トランスコーディング、保留音などで発生する可能性があります。

ほとんどのセキュリティ対応デバイスでは、認証とシグナリングの暗号化がメディア暗号化の最小要件として機能します。つまり、デバイスがシグナリングの暗号化と認証をサポートしていない場合、メディアの暗号化は実行できません。 CiscoIOS ゲートウェイとトランクは、認証なしのメディア暗号化をサポートしています。 CiscoIOS ゲートウェイおよびトランクの場合、SRTP 機能 (メディア暗号化) を有効にする場合、IPSec を設定する必要があります。

警告 ゲートウェイとトランクに SRTP またはシグナリング暗号化を設定する前に、Cisco は強く IPSec を設定することをお勧めします。CiscoIOS MGCP ゲートウェイ、H.323 ゲートウェイ、H.323/H.245/H.225 トランクは IPSec 設定に依存しているため、セキュリティ-関連情報は平文では送信されません。 Unified Communications Manager は、IPSec が正しく設定されているかどうかの確認を行いません。 IPSec を適切に設定しないと、セキュリティ関連の情報が漏えいする可能性があります。

SIP トランクは TLS に依存して、セキュリティ関連情報が平文で送信されないようにします。

次の例では、SCCP および MGCP コールのメディア暗号化を示します。

1. メディアの暗号化と認証をサポートする端末 A と端末 B は、Unified Communications Manager に登録します。
2. デバイス A がデバイス B に発信するとき、Unified Communications Manager はキーマネージャ関数に 2 セットのメディアセッションマスター値を要求します。
3. 両方のデバイスが 2 つのセットを受信します。1 つはメディア ストリーム用のデバイス A - デバイス B で、もう 1 つはメディア ストリーム用のセットである デバイス B - デバイス A です。
4. マスター値の最初のセットを使用して、デバイス A はメディア ストリーム、デバイス A - デバイス B を暗号化および認証するキーを取得します。
5. マスター値の 2 番目のセットを使用して、デバイス A はメディア ストリーム、デバイス B - デバイス A を認証して復号化するキーを取得します。
6. デバイス B は、逆の操作シーケンスでこれらのセットを使用します。
7. デバイスがキーを受信した後、デバイスは必要なキー導出を実行し、SRTP パケット処理が発生します。

（注） SIP および H.323 トランク/ゲートウェイを実行している電話は、独自の暗号化パラメータを生成し、それらを Unified Communications Manager に送信します。

電話会議でのメディア暗号化については、「電話会議リソースの安全性」に関連するトピックを参照してください。

TLS および SIP SRTP の AES 256 暗号化サポート

Cisco コラボレーション ソリューションは、シグナリングとメディア暗号化に Transport Layer Security (TLS) と Secure Real-time Transport Protocol (SRTP) を使用します。 現在、128 ビットの暗号化キーを持つ Advanced Encryption Standard（AES）が暗号化方式として使用されます。 AES はまた、認証方法としてハッシュベースのメッセージ認証コードセキュアハッシュアルゴリズム-1 (HMAC-SHA-1) も使用します。 これらのアルゴリズムは、必要とされる変化するセキュリティとパフォーマンスのニーズを満たすために効果的にスケールすることができません。 高まるセキュリティとパフォーマンスの要件を満たすために、Next-Generation Encryption (NGE) での暗号化、認証、デジタル署名、キー交換のアルゴリズムとプロトコルが開発されました。 また、NGE をサポートする TLS および Session Initiation Protocol (SIP) SRTP では、AES 128 の代わりに AES 256 暗号化サポートが提供されます。

TLS および SIP SRTP の AES 256 暗号化サポートが強化され、シグナリングとメディア暗号化の AES 256 暗号サポートに重視されています。 この機能は、Unified Communications Manager で実行されるアプリケーションが、SHA-2（セキュアハッシュアルゴリズム）標準に準拠し、連邦情報処理標準（FIPS）に準拠している AES-256 ベースの暗号を使用する TLS 1.2 接続をサポートするのに役立ちます。

この機能には次の要件があります。

- SIP トランクおよび SIP 回線が開始する接続。
- Unified Communications Manager が SIP 回線および SIP トランク経由の SRTP 通話に対してサポートする暗号。

（注） このリリースでは、TLS 1.2 は SIP などの一部のインターフェイスでサポートされていますが、すべてのインターフェイスではサポートされていません。 コラボレーションの展開では、TLS 1.0 および 1.1 を有効にしておくことをお勧めします。

TLS での AES 256 および SHA-2 のサポート

Transport Layer Security (TLS) プロトコルは、2 つのアプリケーション間の通信に認証、データ整合性、および機密性を提供します。 TLS 1.2 は Secure Sockets Layer (SSL) プロトコルバージョン 3.0 に基づいていますが、この 2 つのプロトコルには互換性がありません。 TLS は、一方がサーバとして機能し、もう一方がクライアントとして機能するクライアント/サーバモードで動作します。 SSL は、伝送制御プロトコル (TCP) レイヤーとアプリケーションの間のプロトコルレイヤーとして位置付けられ、クライアントとサーバ間の安全な接続を形成し、ネットワーク上で安全に通信できるようにします。 TLS が動作するためには、信頼できるトランスポート層プロトコルとして TCP が必要です。

Unified Communications Manager では、TLS 1.2 の AES 256 および SHA-2 (セキュア ハッシュ アルゴリズム-2) サポートは、SIP トランクと SIP 回線によって開始される接続を処理するための機能強化です。 サポートされている AES 256 および SHA-2 準拠の暗号は以下のとおりです。

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 - 暗号文字列は ECDH-RSA-AES128-GCM-SHA256 です。
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 - 暗号文字列は ECDH-RSA-AES256-GCM-SHA384 です。

引数の説明

- Transport Layer Security（TLS）
- ECDH は楕円曲線 Diffie-Hellman アルゴリズムで、これはアルゴリズムです。
- RSA は Rivest Shamir Adleman と命名されたもので、これはアルゴリズムです。
- AES は高度暗号化標準です
- GCM はガロア/カウンター モードです

新しくサポートされた暗号に加えて、Unified Communications Manager は引き続き TLS_RSA_WITH_AES_128_CBC_SHA をサポートします。 この暗号の暗号文字列は AES128-SHA です。

（注）
- Unified Communications Manager 証明書は RSA に基づいています。
- Unified Communications Manager 10.5 (2) では、Cisco エンドポイント (電話) は上記の新しい暗号を TLS 1.2 でサポートしていません。
- Unified Communications Manager の TLS 1.2 強化での AES 256 および SHA-2 (セキュアハッシュアルゴリズム-2) サポートにより、認証局プロキシ 機能 (CAPF) のデフォルトのキーサイズが 2048 ビットに増加されました。

SRTP SIP コール シグナリングでの AES 256 サポート

Secure Real-time Transport Protocol (SRTP) は、Real-time Transport Protocol (RTP) の音声とビデオのメディア、および対応する Real-time Transport Control Protocol (RTCP) ストリームの両方に対して、機密性とデータの整合性を提供する方法を定義します。 SRTP は暗号化とメッセージ認証ヘッダーを使用してこの方法を実装します。 SRTP では、暗号化は RTP パケットのペイロードにのみ適用され、RTP ヘッダーには適用されません。 ただし、メッセージ認証は RTP ヘッダーと RTP ペイロードの両方に適用されます。 また、メッセージ認証はヘッダー内の RTP シーケンス番号に適用されるため、SRTP はリプレイ攻撃に対する保護を間接的に提供します。 SRTP は暗号化方式として 128 ビット暗号化キーを持つ Advanced Encryption Standards (AES) を使用します。 また、認証方法としてハッシュベースのメッセージ認証コードセキュアハッシュアルゴリズム-1 (HMAC-SHA-1) も使用します。

Unified Communications Manager は、SIP 回線および SIP トランクを介した SRTP 通話の暗号をサポートしています。 これらの暗号は AEAD_AES_256_GCM および AEAD_AES_128_GCM で、AEAD は Authenticated-Encryption with Associated-Data、GCM はガロア/カウンター モードです。 これらの暗号は GCM に基づいています。 これらの暗号がセッション記述プロトコル (SDP) に存在する場合、AES 128 および SHA-1 ベースの暗号と比較して、より高い優先順位で扱われます。 Cisco エンドポイント（電話）は、SRTP 用の Unified Communications Manager に追加するこれらの新しい暗号をサポートしていません。

新しくサポートされた暗号に加えて、Unified Communications Manager は引き続き次の暗号をサポートします。

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 暗号化は、次の通話でサポートされています。

- SIP 回線から SIP 回線へのコール シグナリング
- SIP 回線から SIP トランクへのシグナリング
- SIP トランクから SIP トランクへのシグナリング

Cisco Unified Communications Manager の要件

- SIP トランクおよび SIP 回線接続での TLS バージョン 1.2 のサポートが利用できます。
- TLS 1.2接続が確立されたとき、暗号サポート —TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (暗号文字列 ECDHE-RSA-AES256-GCM-SHA384) および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (暗号文字列 ECDHE-RSA-AES128-GCM-SHA256) が利用できます。 これらの暗号は GCM に基づいており、SHA-2 カテゴリに準拠しています。
- Unified Communications Manager は TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 暗号を使用して TLS1.2 を開始します。 ピアが TLS1.2 をサポートしない場合、Unified Communications Manager は既存の AES128-SHA 暗号を使用する TLS 1.0 にフォールバックします。
- SIP 回線および SIP トランク上の SRTP 通話は、GCM ベースの AEAD_AES_256_GCM および AEAD_AES_128_GCM 暗号をサポートします。

連携動作と制限事項

- Unified Communications Manager の要件は、SIP 回線と SIP トランク、および基本的な SIP から SIP への通話のみに適用されます。
- SIP 以外のプロトコルに基づくデバイス タイプは、サポートされている暗号を使用した TLS バージョンの既存の動作を引き続きサポートします。 また、Skinny Call Control Protocol (SCCP) は、以前サポートされていた暗号の TLS 1.2 もサポートしています。
- SIP から SIP 以外への通話では、引き続き AES 128 および SHA-1 ベースの暗号が使用されます。

AES 80 ビット認証サポート

Unified Communications Manager は、保留音 (MOH)、音声自動応答 (IVR)、アナンシエータで暗号化暗号として使用される 128 ビットの暗号化キーと 80 ビットの認証タグを含む Advanced Encryption Standard (AES) をサポートします。 デフォルトでは、80 ビット認証タグをサポートする電話は、AES_CM_128_HMAC_SHA1_80暗号を使用して、MOH、IVR、アナンシエータを再生します。

電話が IP 音声メディアストリーミング（IPVMS）で安全に接続する場合、AES_CM_128_HMAC_SHA1_80 暗号が優先されます。 電話が 80 ビット認証をサポートしていない場合、AES_CM_128_HMAC_SHA1_32 暗号に戻ります。 電話が 80 ビットまたは 32 ビットの認証タグをサポートしていない場合、ネゴシエーションは Real-Time Transport Protocol (RTP) 経由で発生します。

（注） SCCP 電話は 32 ビット認証タグのみをサポートします。 そのため、電話と IPVMS 間のネゴシエーションは AES_CM_128_HMAC_SHA1_32 暗号でのみ発生します。

電話 A が AES_CM_128_HMAC_SHA1_80 をサポートし、電話 B が AES_CM_128_HMAC_SHA1_32 暗号をサポートし、ユーザー A（電話 A）がユーザー B（電話 B）にダイヤルし、コールがユーザー B によって保留にされると、電話 A は MOH に接続します。 電話 A は 80 ビット認証タグのみをサポートするため、電話 A と MOH の間のネゴシエーションは AES_CM_128_HMAC_SHA1_80 暗号を通じて発生します。

ユーザー B（電話 B）がユーザー A（電話 A）にダイヤルし、ユーザー A によりコールが保留状態になった場合、電話 B は 32 ビット認証タグのみをサポートするため、電話 B と MOH の間のネゴシエーションは AES_CM_128_HMAC_SHA1_32 暗号によって発生します。

電話が 80 ビット認証タグをサポートする場合、電話と IVR または Annunciator 間のネゴシエーションは AES_CM_128_HMAC_SHA1_80 を通じて発生します。

次の表は、電話機とその交渉暗号でサポートされている暗号を示しています。

表 *4:* 電話機能と交渉暗号

電話機能	交渉暗号
AES_CM_128_HMAC_SHA1_32 および AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32	AES_CM_128_HMAC_SHA1_32
AES_CM_128_HMAC_SHA1_80	AES_CM_128_HMAC_SHA1_80
AES_CM_128_HMAC_SHA1_32 および AES_CM_128_HMAC_SHA1_80 以外	RTP に戻します。

自己暗号化ドライブ

Unified Communications Manager は、自己暗号化ドライブ (SED) をサポートしています。 これはフルディスク暗号化 (FDE) とも呼ばれます。 FDE は、ハードドライブ上で利用可能なすべてのデータを暗号化するために使用される暗号化方法です。 このデータには、ファイル、オペレーティング システム、およびソフトウェア プログラムが含まれます。 ディスク上で利用できるハードウェアは、すべての受信データを暗号化し、すべての送信データを復号化します。

ドライブがロックされると、暗号化キーが作成され、内部に保存されます。 このドライブに保存されているすべてのデータは、そのキーを使用して暗号化され、暗号化された形式で保存されます。 FDE はキー ID とセキュリティキーで構成されています。

詳細については、『Cisco UCS C-Series サーバ統合管理コントローラ GUI 構成ガイド』を参照してください。

構成ファイルの暗号化

Unified Communications Managerは、ダイジェスト資格情報や管理者パスワードなどの機密データを、TFTPサーバからダウンロードされた構成ファイルの電話機にプッシュします。

Unified Communications Managerは、データベース内でこれらの資格情報を保護するために、可逆的な暗号化を使用しています。 ダウンロード プロセス中にこのデータを保護するために、Cisco では、このオプションをサポートするすべての Cisco IP 電話に対して、暗号化構成ファイルを構成することを推奨しています。 このオプションが有効な場合、デバイス構成ファイルのみがダウンロード用に暗号化されます。

（注） 状況によっては、機密データを暗号化されていない状態で電話にダウンロードすることを選択することもできます。たとえば、電話のトラブルシューティング時。

Unified Communications Manager は暗号化キーをエンコードし、データベースに保存します。TFTP サーバは、対称暗号化キーを使用して、構成ファイルを暗号化し、解読します。

- 電話に PKI 機能がある場合、 Unified Communications Manager は電話の公開鍵を使用して、電話構成ファイルを暗号化できます。
- 電話が PKI 機能を持たない場合、 Unified Communications Manager と電話で一意の対称キーを設定する必要があります。

Unified Communications Manager Administrationの[電話セキュリティプロファイル]ウィンドウで暗号化設定ファイルを有効にします。その後、[電話の設定]ウィンドウで設定した設定を電話に適用します。

デフォルトのセキュリティ管理タスク

以下はデフォルトのセキュリティ管理タスクです。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Unified IP Phone の ITL ファイルの更新	TFTP 構成ファイルを検証します。
ステップ 2	デフォルトのセキュリティに対するエンドポイントサポートを取得する	Cisco Unified IP Phone サポートリストページを Cisco Unified レポートを使用して取得します。
ステップ 3	クラスタを 8.0 より前のリリースにロールバックする	クラスターのロールバックを準備します。

	コマンドまたはアクション	目的
ステップ 4	ITL ファイルの一括リセットの実行 （33 ページ）	ITL ファイルの一括リセットを実行します。
ステップ 5	CTL ローカルキーのリセット	CLI コマンドで Cisco Trust List (CTL) ファイルのリセットを実行します
ステップ 6	ITLRecovery 証明書の有効期間を表示します	ITLRecovery 証明書の有効期間を表示します。
ステップ 7	認証と暗号化を設定します	新規インストールに認証と暗号化を実装する。

Cisco Unified IP Phones の ITL ファイルの更新

電話に ITL ファイルがインストールされた状態で [デフォルトのセキュリティ] を使用する Unified Communication Manager による一元化された TFTP は TFTP 構成ファイルを検証しません。

リモート クラスタからの電話が集中型 TFTP 展開に追加される前に、次の手順を実行します。

手順

ステップ 1 中央の TFTP サーバーで、エンタープライズパラメータ **Preparecluster for pre CM-8.0 ロールバック**を有効にします。

ステップ 2 TVS および TFTP を再起動します。

ステップ 3 すべての電話をリセットして、ITL 署名検証を無効にする新しい ITL ファイルがダウンロードされたことを確認します。

ステップ 4 HTTPS の代わりに HTTP を使用するようにエンタープライズ パラメータ セキュア https URL を設定します。

（注）
Unified Communications Manager リリース 10.5 以降では、[**CM-8.0 以前のロールバック用にクラスタを用意する**] パラメータを有効にすると、電話が自動的にリセットされます。 中央TFTP サーバの Unified Communications Manager バージョンおよびこのパラメータを有効にする方法については、 Cisco Unified Communications Manager セキュリティガイドの「8.0 以前のリリースへのクラスタのロールバック」を参照してください。

Cisco Unified IP Phone サポートリストの取得

Cisco Unified Reporting ツールを使用して、デフォルトでセキュリティをサポートする Cisco エンドポイントのリストを生成します。

手順

ステップ 1 Cisco Unified Reporting から、 **システムレポートを選択します。**

ステップ 2 **[システムレポート]** リストから、 **Unified CM 電話機能リストを選択します。**

ステップ 3 **[製品]** ドロップダウンリストから、 **デフォルトのセキュリティ** を選択します。

ステップ 4 [送信（Submit）]をクリックします。
特定の電話でサポートされている機能のリストを含むレポートが生成されます。

クラスタを 8.0 より前のリリースにロールバックする

Unified Communications Managerの 8.0 より前のリリースにクラスターをロールバックする前に、pre-8.0へのロールバックのためのクラスターの準備エンタープライズパラメータを使用して、ロールバックするクラスターを準備する必要があります。

クラスターのロールバックを準備するには、クラスター内の各サーバでこの手順に従います。

手順

ステップ 1 Unified Communications Managerから **[システム]** > **[エンタープライズパラメータ設定]**を選択します。

エンタープライズパラメータ設定 ウィンドウが表示されます。

Prepare Cluster for Rollback to pre-8.0 えんたーぷらいず パラメータを **True** に設定します。

（注）
クラスタを Unified Communications Manager の pre-8.0 リリースにロールバックする準備をしている場合にのみ、このパラメータを有効にしてください。 このパラメータが有効になっている間、https を使用する電話サービス (エクステンション モビリティなど) は機能しません。 ただし、このパラメータが有効になっている間も、ユーザは基本的な通話を発信および受信し続けることができます。

ステップ 2 Cisco IP Phonesが自動的に再起動し、Unified Communications Manager に登録するまで 10 分間待ちます。

ステップ 3 クラスター内の各サーバを前のリリースに戻します。

クラスタを以前のバージョンに戻す方法の詳細については、 *Cisco Unified Communications Manager* 管理ガイドを参照してください。

ステップ 4 クラスターが前のバージョンへの切り替えを完了するまで待ちます。

ステップ 5 以下のいずれかのリリースを混合モードで実行している場合、CTL クライアントを実行する必要があります。

- Unified Communications Manager720 リリース
  - 7.1(2)のすべての通常リリース
  - 712のすべてのESリリースは007.001(002.32016.001)より前です
- Unified Communications Manager リリース 7.1 (3)
  - 713のすべての通常リリースは007.001(003.21900.003) = 7.1(3a)su1aより前です
  - 712のすべてのESリリースは007.001(003.21005.001)より前です

（注）
CTL クライアントの実行についての詳細は、「「CTL クライアントの設定」」の章を参照してください。

ステップ 6 [「8.0より前にロールバックするためのクラスターの準備]が[エンタープライズパラメータ]でTrueに設定されている場合、企業ディレクトリを機能させるには、次の変更を行う必要があります。」

[**デバイス] >デバイス設定 >電話サービス >企業ディレクトリ** では、サービスの URL を Application:Cisco/CorporateDirectory から http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp に変更する必要があります。

ステップ 7 [「8.0より前にロールバックするためのクラスターの準備]が[エンタープライズパラメータ]でTrueに設定されている場合、企業ディレクトリを機能させるには、次の変更を行う必要があります。」

端末 >デバイスの設定 >電話サービス >パーソナルディレクトリ サービスの URL を、Application:Cisco/PersonalDirectory から、'http://<ipaddr>>:8080/ccmpd/pdCheckLogin.do?name=未定義に変更する必要があります。

元に戻した後にリリース 8.6 以降に切り替える

クラスタをリリース 7.x に戻した後で、リリース 8.6 以降のパーティションに戻す場合は、この手順に従ってください。

手順

ステップ 1 クラスターを非アクティブパーティションに戻すための手順に従います。 詳細については、『*Cisco Unified Communications Manager* 管理ガイド』を参照してください。

ステップ 2 以下のリリースのいずれかを混合モードで実行していた場合、CTLクライアントを実行する必要があります。

Unified Communications Manager リリース 7.1(2)

- 7.1(2)のすべての通常リリース
- 712のすべてのESリリースは007.001(002.32016.001)より前です
- Unified Communications Manager リリース 7.1(3)
  - 713のすべての通常リリースは007.001(003.21900.003) = 7.1(3a)su1aより前です
  - 712のすべてのESリリースは007.001(003.21005.001)より前です

（注）
CTL クライアントの実行についての詳細は、「「CTL クライアントの設定」」の章を参照してください。

ステップ 3 Unified Communications Manager Administration で、**[システム（System）] > [エンタープライズパラメータ（Enterprise Parameters）]** を選択します。

エンタープライズパラメータ設定 ウィンドウが表示されます。

Prepare Cluster for Rollback to pre-8.6 えんたーぷらいず パラメータを **True** に設定します。

ステップ 4 Cisco Unified IP Phone が自動的に再起動し、Unified Communications Manager に登録するまで 10 分ほど待ちます。

ITL ファイルの一括リセットの実行

この手順は必ず Unified Communications Manager パブリッシャから実行してください。

ITL ファイルの一括リセットは、電話が ITL ファイルの署名者を信頼しなくなり、ローカルの TFTP サービスまたは TVS を使用して提供される ITL ファイルを認証できない場合に実行されます。

一括リセットを実行するには、CLI コマンド **utils itl reset** を使用します。 このコマンドは新しいITL回復ファイルを生成し、電話とCUCM上のTFTPサービスの間の信頼を再確立します。

ヒント Unified Communications Manager をインストールする場合、CLI コマンド **file get tftp***ITLRecovery.p12*を使用して ITL 復旧ペアをエクスポートし、DRを通じてバックアップを実行します。SFTP サーバー（キーがエクスポートされる場所）とパスワードの入力も求められます。

手順

ステップ 1 次のいずれかの手順を実行します。

- **utils itl reset localkey** を実行します。
- **utils itl reset remotekey** を実行します。

（注）
utils itl reset localkey の場合、ローカルキーはパブリッシャーに存在します。 このコマンドを発行すると、ITL ファイルは ITL 回復キーがリセットされる間、CallManager キーによって一時的に署名されます。

ステップ 2 **show itl** を実行してリセットが成功したことを確認します。

ステップ 3 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 4 [**リセット**（**Reset**）] をクリックします。

デバイスが再起動します。 これで、CallManager キーで署名された ITL ファイルをダウンロードし、構成ファイルを受け入れる準備ができました。

ステップ 5 TFTP サービスを再起動し、すべてのデバイスを再起動します。

（注）
TFTP サービスを再起動すると、ITL ファイルが ITLRecovery キーで署名され、ステップ 1 の変更がロールバックされます。

デバイスは、ITLRecovery キーで署名された ITL ファイルをダウンロードし、Unified Communications Manager に再度正しく登録します。

CTL ローカルキーのリセット

Unified Communications Manager クラスタ上のデバイスがロックされ、信頼できるステータスを失った場合、CLI コマンド **utils ctl reset localkey を使用して Cisco Trust List (CTL) ファイルのリセットを実行します。** このコマンドにより新しい CTL ファイルが生成されます。

手順

ステップ 1 **utils ctl reset localkey** を実行します。

（注）
utils ctl reset localkey の場合、ローカルキーはパブリッシャーに存在します。 このコマンドを発行するとき、CTL ファイルは一時的に CallManager キーによって署名されます。

ステップ 2 **show ctl** を実行してリセットが成功したことを確認してください。

ステップ 3 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。
[**エンタープライズパラメータの設定**] ページが表示されます。

ステップ 4 [**リセット（Reset）**] をクリックします。

デバイスが再起動します。 これで、CallManager キーで署名された CTL ファイルをダウンロードし、構成ファイルを受け入れる準備が整いました。

ステップ 5 **utils ctl update CTLFile** を実行し、必要なサービスを再起動してステップ 1 の変更をロールバックします。

デバイスが再起動します。 これで、CallManager キーで署名された CTL ファイルをダウンロードし、構成ファイルを受け入れる準備が整いました。

デバイスは、必要なキーを使用して署名された CTL ファイルをダウンロードし、再度 Unified Communications Manager に登録します。

ITLRecovery 証明書の有効期間を表示する

ITLRecovery 証明書は、電話に対して長い有効期間を持っています。 [**証明書ファイルのデータ**] ペインに移動すると、有効期間やその他の ITLRecovery 証明書の詳細を表示できます。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

ステップ 2 検索パラメータを入力して、証明書を検索して設定の詳細を表示します。
基準に一致する証明書の一覧が **証明書リスト** ページに表示されます。

ステップ 3 有効期間を表示するには、 **ITLRecovery** リンクをクリックしてください。

ITLRecovery 証明書の詳細は **証明書ファイルのデータ** ペインに表示されます。

有効期間は現在の年から20年間です。

認証と暗号化のセットアップ

重要 この手順は CTL クライアント暗号化オプションに適用されます。 **utils ctl** CLI コマンドセットを使用して暗号化をセットアップすることもできます。 CLI の使用の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

以下の手順は、認証と暗号化を実装するために実行する必要があるすべてのタスクを示しています。指定されたセキュリティ機能のために実行する必要がある作業が記載されている章の参照については、関連トピックを参照してください。

- 新規インストールに認証と暗号化を実装するには、次の表を参照してください。
- セキュアなクラスタにノードを追加するには、「インストール *Cisco Unified Communications Manager*」を参照してください。新しいノードの追加方法と新しいノードのセキュリティ設定方法について説明しています。

手順

ステップ 1 Cisco CTL Provider サービスを有効にします。 Cisco Unified Serviceability

クラスタ内の各 Unified Communications Manager サーバで Cisco CTL Provider サービスを有効にしてください。

ヒント
Unified Communications Manager アップグレード前にこのサービスをアクティベート済みの場合は、再度アクティベートする必要はありません。サービスはアップグレード後に自動的にアクティベートされます。

ステップ 2 Cisco Unified Serviceability で Cisco Certificate Authority Proxy サービスを有効にして、ローカルで有効な証明書をインストール、アップグレード、トラブルシューティング、または削除します。

最初のノードのみで Cisco Certificate Authority Proxy サービスを有効にします。

ワンポイント アドバイス
Cisco CTL クライアントをインストールして設定する前にこのタスクを実行することで、CAPF を使用するために CTL ファイルを更新する必要がなくなります。

ステップ 3 デフォルトのポート設定を使用しない場合は、TLS 接続用のポートを構成します。

ヒント
Unified Communications Manager これらの設定をアップグレード前に行った場合、その設定はアップグレード中に自動的に移行されます。

ステップ 4 暗号化に Cisco CTL クライアントを使用する場合、少なくとも 2 つのセキュリティトークンと、Cisco CTL クライアントに設定するサーバのパスワード、ホスト名/IP アドレス、およびポート番号を取得します。

（注）
utils ctl CLI オプションにはハードウェア セキュリティ トークンは必要ありません。

ステップ 5 Cisco CTL クライアントをインストールします。

ヒント

この Unified Communications Manager リリースへのアップグレード後に Cisco CTL ファイルを更新するには、この Cisco Unified Communications Manager Administration リリースで利用できるプラグインをインストールする必要があります。

ステップ 6 Cisco CTL クライアントを設定します。

ヒント
Unified Communications Manager アップグレードの前に Cisco CTL ファイルを作成している場合、Cisco CTL ファイルはアップグレード中に自動的に移行されます。 このリリース Unified Communications Manager へのアップグレード後に Cisco CTL ファイルを更新するには、Cisco CTL クライアントの最新バージョンをインストールして設定する必要があります。

（注）
Cisco の CTL クライアントは Release 14 からサポートされなくなりました。Cisco CTL プラグインの代わりに、CLI コマンドを使用して Unified Communications Manager サーバを混合モードに切り替えることを推奨します。

ステップ 7 電話セキュリティ プロファイルを設定します。

プロファイルを構成する際には、以下のタスクを実行します。

a) デバイス セキュリティ モードを構成します。

ヒント
デバイスのセキュリティモードは Unified Communications Manager アップグレード中に自動的に移行されます。 以前のリリースで認証のみをサポートしていた端末の暗号化を設定する場合は、[**電話の設定**] ウィンドウで暗号化のセキュリティプロファイルを選択する必要があります。

b) CAPF 設定を構成します (SCCP および SIP を実行している一部の電話用)。

追加の CAPF 設定が [電話の設定] ウィンドウに表示されます。

c) SIP を実行している電話にダイジェスト認証を使用する予定の場合は、[ダイジェスト認証を有効にする] チェックボックスをオンにします。
d) 暗号化された構成ファイルを有効にするには (SCCP および SIP を実行している一部の電話用)、[暗号化された設定ファイル] チェックボックスをオンにします。
e) 構成ファイルのダウンロードからダイジェスト資格情報を除外するには、[構成ファイルからダイジェスト資格情報を除外する] チェックボックスをオンにします。

ステップ 8 電話セキュリティ プロファイルを電話に適用します。

以下の手順は任意です。

ステップ 9 （任意） ローカルで有効な証明書がサポートされている Cisco Unified IP 電話 にインストールされていることを確認してください。

ステップ 10 （任意） SIP を実行している電話のダイジェスト認証を設定してください。

ステップ 11 （任意） 電話強化タスクを実行してください。

ヒント

Unified Communications Manager をアップグレードする前に電話強化の設定を行った場合、デバイス構成の設定はアップグレード中に自動的に移行されます。

ステップ 12 （任意） セキュリティのために電話会議ブリッジのリソースを構成します。

ステップ 13 （任意） セキュリティのためにボイスメール ポートを設定します。

詳細については、該当する Cisco Unity または Cisco Unity Connection インテグレーションガイドを Unified Communications Manager リリースで参照してください。

ステップ 14 （任意） SRST 参照のセキュリティ設定を構成します。

ヒント
前の Unified Communications Manager リリースでセキュアな SRST 参照を設定した場合、 Unified Communications Manager アップグレード中に自動的に移行します。

ステップ 15 （任意） IPSec を設定します。

詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。

ステップ 16 （任意） SIP トランク セキュリティ プロファイルを設定します。

ダイジェスト認証を使用する予定の場合は、プロファイルの[ダイジェスト認証を有効にする] チェックボックスをオンにします。

トランクレベル認証の場合、許可された SIP 要求の認証チェックボックスを選択します。

トランクレベルの認証の後にアプリケーションレベルの認証を行う場合は、[アプリケーションレベルの認証を有効にする] チェックボックスをオンにします。

ダイジェスト認証がチェックされていない限り、アプリケーション レベルの認証をチェックすることはできません。

ステップ 17 （任意） トランクに SIP トランク セキュリティ プロファイルを適用します。

ステップ 18 （任意） トランクのダイジェスト認証を設定します。

ステップ 19 （任意） SIP トランク セキュリティ プロファイルで [アプリケーション レベルの認証を有効にする] チェックボックスをオンにした場合、[アプリケーション ユーザの構成] ウィンドウの認証チェックボックスをオンにして、許可される SIP 要求を設定します。

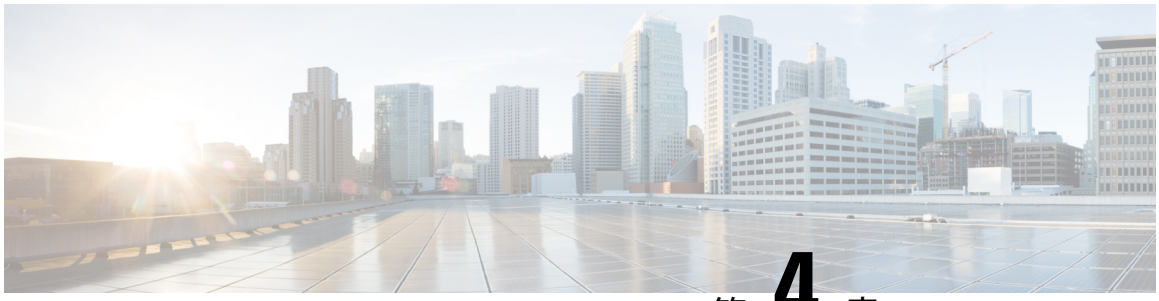
ステップ 20 （任意） すべての電話をリセットします。

ステップ 21 （任意） すべてのサーバを再起動します。

第 II 部

基本システムセキュリティ

- 証明書 （41 ページ）
- セキュリティモード （73 ページ）
- 暗号管理 （79 ページ）
- 安全なトーンとアイコン （95 ページ）
- Certificate Authority Proxy 機能 （105 ページ）
- TFTP 暗号化 （123 ページ）
- 電話機のセキュリティ （131 ページ）
- セキュアな電話会議リソースのセットアップ （169 ページ）
- ボイスメッセージ ポートのセキュリティ設定 （185 ページ）
- トランクおよびゲートウェイ SIP セキュリティ （191 ページ）
- Cisco CTL クライアントのセットアップ （209 ページ）
- TLS セットアップ （227 ページ）



第 4 章

証明書

- 証明書の管理 （41 ページ）
- 証明書の監視と失効 （68 ページ）

証明書の管理

証明書管理機能では、さまざまな証明書タイプ、証明書の管理に関連するタスク、および証明書の監視と失効の方法の概要を提供します。

証明書の概要

証明書は展開で安全な接続を確立するために重要です。 ネットワーク上の個人、コンピュータ、その他のサービスを認証します。 証明書管理を実装することで、複雑さを軽減しながら、優れたレベルの保護を提供できます。

証明書は証明書の所有者のアイデンティティを証明するファイルで、次の情報が含まれています。

- 証明書所有者名
- [パブリックキー(Public Key)]
- 証明書を発行した認証局のデジタル署名

Unified Communications Manager は、公開鍵基盤 (PKI) の証明書を使用して暗号化を有効にし、サーバとクライアントのアイデンティティを検証します。 適切な信頼ストアに一致する証明書がない限り、他のシステムを信頼せず、アクセスを拒否します。

ルート証明書は、デバイスとアプリケーションユーザを含む、ユーザとホストの間の接続を保護します。 証明書はクライアントとサーバのアイデンティティを保護し、ルート トラスト ストアに追加します。

管理者は、サーバ証明書の指紋の表示、自己署名証明書の再生成、およびUnified Communications Manager インターフェイスからの信頼できる証明書の削除を行うことができます。 また、CLI を使用して自己署名証明書を再生成して表示することもできます。

Unified Communications Manager 信頼ストアの更新および証明書の管理についての詳細は、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

（注） Unified Communications Manager は、PEM (.pem) および DER (.der) 形式の証明書のみをサポートします。 DER または PEM でサポートされる証明書の最大サイズは 4096 ビットです。

（注） Unified Communications Manager は、ワイルドカード エントリを含む証明書をサポートしていません。 たとえば、"*.cisco.com"。

（注） Unified Communications Manager トラストストアに期限切れの証明書がある場合、これらの証明書はリリース 12.5(1)SU6 および 14SU2 以降へのアップグレード中にインポートされません。

2 つの証明書をアップロードする場合、名前と有効期間が同じであることを確認し、シリアル番号と署名アルゴリズムが異なることを確認してください。

例:

ルート CA `27:20:41:0c:5b:08:69:80:42:62:4f:13:bd:16:06:6a` シリアル番号および SHA-1 アルゴリズムは Unified Communications Manager tomcat-trust に存在します。

`7b:35:33:71:0b:7c:08:b2:47:b3:aa:f9:5c:0d:ca:e4` シリアル番号および SHA-256 アルゴリズムの証明書をアップロードしようとすると、証明書の管理:

- 受け取った証明書の有効性を確認します
- Tomcat trust フォルダから同じ名前の証明書を検索します
- Tomcat trust フォルダーにある証明書のシリアル番号と、アップロードしている受信した証明書を比較します

シリアル番号が異なる場合、両方の証明書の有効開始日を確認します。 新しい受信証明書の開始タイムスタンプが最新の場合、既存の証明書を置換し、それ以外の場合はアップロードされません。

SHA-1 および SHA-256 アルゴリズムには同じサブジェクト名または共通名があります。これは、同じエンティティに属していることを意味します。 Unified Communications Manager フレームワークは、Unified Communications Manager のサーバー上でこれら両方のアルゴリズムを同時にサポートすることはできません。 署名アルゴリズムに関係なく、特定の信頼フォルダー内のエンティティに属する 1 つの証明書のみをサポートします。

証明書の種類

このセクションでは、さまざまなタイプの証明書と証明書署名要求のキー使用拡張機能の概要について説明します。

電話の証明書タイプ

電話証明書は、電話を認証する一意の識別子です。 これはIP攻撃に対するセキュリティにとって非常に重要です。

電話証明書は次のとおりです。

表 *5:*

電話証明書	説明
製造元でインストールされる証明書（MIC）	MIC は Cisco マニュファクチャリング CA によって署名されており、サポートされている [適切な用語を挿入] Cisco Unified IP 電話にはこの証明書が自動的にインストールされます。 MIC は、ローカルで有効な証明書 (LSC) のインストールのために Cisco 認証局プロキシ機能 (CAPF) で認証するか、暗号化された構成ファイルをダウンロードします。 管理者は証明書を変更、削除、失効させることができないため、有効期限が切れた後は [適切な主語を挿入]を使用できません。
ローカルで有効な証明書 (LSC)	Cisco Unified IP 電話は、セキュアモードで動作するためにLSCが必要であり、認証と暗号化に使用されます。 CAPF オンラインまたはオフライン CA によって署名され、MIC より優先されます。 CAPF に関連する必要なタスクを実行した後、この証明書はサポートされている電話にインストールされます。 認証または暗号化にデバイスセキュリティモードを設定すると、LSC により Unified Communications Manager と電話間の接続が保護されます。

ヒント LSC のインストールには、MICのみを使用することをお勧めします。 TLS 接続を認証するために LSC をサポートしています Unified Communications Manager。 電話設定が TLS 認証またはその他の目的で MIC を使用する場合、MIC ルート証明書は簡単に危険にさらされるため、当社は責任を負いません。

Cisco Unified IP 電話の 6900、7900、8900、9900 シリーズをアップグレードして TLS 接続に LSC を使用するように Unified Communications Manager。 互換性の問題を避けるため、 Unified Communications Manager 信頼ストアから MIC ルート証明書を削除してください。

（注） MIC を使って Unified Communications Manager への TLS 接続を行う電話モデルでは、登録ができない場合があります。

管理者は次の MIC ルート証明書を Unified Communications Manager 信頼ストアから削除する必要があります:

- CAP-RTP-001
- CAP-RTP-002
- Cisco_Manufacturing_CA
- Cisco_Root_CA_2048
- Cisco_Manufacturing_CA_SHA2
- Cisco_Root_CA_M2
- ACT2_SUDI_CA

CAPF 信頼ストアに残る MIC ルート証明書は、証明書のアップグレードに使用されます。Unified Communications Manager 信頼ストアの更新と証明書の管理については、 Cisco Unified Communications Manager アドミニストレーション ガイド を参照してください。

（注） Unified Communications Manager リリース 12.5.1SU2 以前では、CallManager-trust ストアから Cisco製造元の証明書を削除すると、セキュアオンボーディング機能が機能しません。これは、電話機から製造時にインストールされた証明書 (MIC) を検証できないためです。 ただし、この機能は Unified Communications Manager リリース 12.5.1SU3 以降で動作します。電話からの MIC を検証するために CAPF 信頼ストアを使用するためです。

サーバ証明書の種類

サーバ証明書は基本的にサーバを識別するためのものです。 サーバ証明書は、コンテンツの暗号化と復号化の目的としています。

Unified Communications Manager サーバ内の自己署名 (自分の) 証明書のタイプは次の通りです:

Unified Communications Manager は次の証明書タイプを Unified Communications Manager トラストストアにインポートします:

表 *6 :* 証明書のタイプと説明

証明書タイプ	説明
Cisco Unity サーバまたは Cisco Unity Connection 証明書	Cisco Unity および Cisco Unity Connection この自己署名ルート証明書を使用して、 Cisco Unity SCCP および Cisco Unity Connection SCCP デバイス証明書を署名します。 Cisco Unity の場合、Cisco Unity テレフォニー統合マネージャ（UTIM）がこの証明書を管理します。 Cisco Unity Connection について、 この証明書は Cisco Unity Connection Administration が管理します。
Cisco Unity および Cisco Unity Connection SCCP デバイス証明書	Cisco Unity および Cisco Unity Connection SCCP デバイスは、この署名付き証明書を使用して、 Unified Communications Manager との TLS 接続を確立します。
SIP プロキシ サーバ証明書	SIP トランク経由で接続する SIP ユーザ エージェントは、 Unified Communications Manager CallManager の信頼ストアに SIP ユーザエージェント証明書が含まれていて、かつSIPユーザエージェントの信頼ストアに Unified Communications Manager 証明書が含まれている場合に認証を行います。

（注） 証明書名は、ボイスメール サーバ名に基づく、証明書のサブジェクト名のハッシュを表します。すべてのデバイス(またはポート)には、ルート証明書をルートとする証明書が発行されます。

以下の追加のトラストストアが存在します。

- Tomcat およびウェブアプリケーションの共通トラストストア
- IPSec-trust
- CAPF 信頼
- ユーザライセンスの信頼性
- TVSの信頼性
- 電話とSAST間の信頼性
- 電話とCTL間の信頼性

Cisco Unity Connection の CA 信頼証明書の詳細については、『Cisco Unified Communications Managerアドミニストレーションガイド』を参照してください。 これらの信頼証明書は、メール、カレンダー情報、または連絡先を取得するための Exchange または Meeting Place Express への接続を保護します。

サードパーティ CA 署名証明書

CA 署名付き証明書は、デジタル証明書に署名して発行する、信頼できるサードパーティの証明書です。

デフォルトでは、 Unified Communications Manager はすべての接続に自己署名証明書を使用します。 しかし、証明書に署名するようにサードパーティ CA を設定することで、セキュリティを追加することができます。 サードパーティ CA を使用するには、Cisco Unified Communications Manager Administration に CA ルート証明書チェーンをインストールします。

CA が署名した証明書を発行するには、CSR を送信して、CA が証明書を発行して署名できるようにします。 証明書をアップロード、ダウンロード、表示する方法の詳細は、 **自己署名証明書** のセクションを参照してください。

設定

Unified Communications Managerに接続する別のシステムから CA 署名付き証明書を使用する場合は、 Cisco Unified Communications Manager Administration で次の操作を行います:

- 証明書に署名した CA のルート証明書チェーンをアップロードします。
- 他のシステムから CA 署名付き証明書をアップロードします。

Unified Communications Managerで CA 署名付き証明書を使用する場合:

- CSR を完成させ、 Cisco Unified Communications Manager Administrationで CA 署名付き証明書を要求します。
- CA ルート証明書チェーンと CA 署名付き証明書の両方をダウンロードしてください Cisco Unified Communications Manager Administration
- CA ルート証明書チェーンと CA 署名付き証明書の両方をアップロードします。

CA のルート証明書を取得および設定する方法の詳細については、Certificate Authorityのドキュメントを参照してください。

外部 CA からの証明書のサポート

Unified Communications Manager は、 Unified Communications Manager GUI からアクセス可能な PKCS#10 証明書署名リクエスト (CSR) メカニズムを使用することで、サードパーティの認証局 (CA) との統合をサポートしています。

現在サードパーティ CA を使用している顧客は、以下の証明書を発行するために CSR メカニズムを使用すべきです。

- Unified Communications Manager
- CAPF
- IPSec
- Tomcat
- TVS

（注） マルチサーバ (SAN) の CA 署名付き証明書は、証明書がパブリッシャーにアップロードされると、クラスター内のノードに適用されますのみ。 新しいマルチサーバ証明書を生成します。新しいノードを追加するか、再構築するたびに、マルチサーバ証明書をクラスターにアップロードします。

システムを混合モードで実行している場合、一部のエンドポイントでは 4096 以上のキーサイズでは CA 証明書を受け付けない場合があります。 混在モードで CA 証明書を使用するには、以下のいずれかのオプションを選択します。

- 証明書キーサイズが4096未満の証明書を使用してください。
- 自己署名証明書の場合：

（注） サードパーティの CA 署名付き証明書をプラットフォームにアップロードして CTL ファイルを更新した後は、必ず CTL クライアントを実行してください。

CTL クライアントを実行した後、更新のために適切なサービスを再起動してください。

次に例を示します。

- Unified Communications Manager 証明書を更新したときには、TFTP サービスと Unified Communications Manager サービスを再起動します。
- CAPF 証明書を更新したら CAPF を再起動します。

Unified Communications Manager または CAPF 証明書をアップロードした後、電話が ITL ファイルを更新するために自動的にリセットされるのを確認できます。

プラットフォームでの証明書署名リクエスト CSR の生成については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

証明書署名要求のキー用途拡張

次の表に、Unified Communications Manager と IM and Presence Service の CA 証明書の両方に対する証明書署名要求（CSR）の主な使用法の拡張を示します。

表 *7 : Cisco Unified Communications Manager CSR* キー鍵用途拡張

	マルチサーバー	拡張キーの使用状況			キーの使用法				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号化	鍵証明書サイン	鍵共有
CallManager CallManager-ECDSA	Y	Y	Y		Y	Y	Y		

	マルチサーバー	拡張キーの使用状況			キーの使用法				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号化	鍵証明書サイン	鍵共有
CAPF（パブリッシャーのみ）	N	Y			Y	N		Y	
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		
TVS	N	Y	Y		Y	Y	Y		

表 *8 : IM and Presence Service* の *CSR* キーの用途の拡張

	マルチサーバー	拡張キーの使用状況			キーの使用法				
		サーバ認証 (1.3.6.1.5.5.7.3.1)	クライアント認証 (1.3.6.1.5.5.7.3.2)	IP セキュリティ末端システム (1.3.6.1.5.5.7.3.5)	デジタル署名	鍵の暗号化	データの暗号化	鍵証明書サイン	鍵共有
cup cup-ECDSA	N	Y	Y	Y	Y	Y	Y		
cup-xmpp cup-xmpp-ECDSA	Y	Y	Y	Y	Y	Y	Y		
cup-xmpp-s2s cup-xmpp-s2s-ECDSA	Y	Y	Y	Y	Y	Y	Y		
ipsec	N	Y	Y	Y	Y	Y	Y		
tomcat tomcat-ECDSA	Y	Y	Y		Y	Y	Y		

（注） 「データの暗号化」ビットは、CA 署名証明書の処理中に変更も削除もされません。

証明書のタスク

このセクションでは、証明書を管理するためのすべての手順が記載されています。

証明書の一括エクスポート

古いクラスターと新しいクラスターが同時にオンラインの場合、証明書の一括移行方法を使用できます。

Cisco Unified IP Phone は、ITL ファイルに対して、または ITL ファイルに存在する TVS サーバに対して、ダウンロードされたすべてのファイルを検証することに注意してください。電話を新しいクラスタに移動する必要がある場合、新しいクラスタが提供する ITL ファイルは、古いクラスタ TVS 証明書ストアによって信頼されている必要があります。

（注） 一括証明書のエクスポート方法は、電話が移行されている間に両方のクラスターがネットワーク接続でオンラインの場合にのみ機能します。

（注） 証明書の一括インポート中、Cisco Extension Mobility Cross Cluster (EMCC) が機能し続けるためには、訪問先クラスタとホーム クラスタの両方で追加の ITLRecovery 証明書をインポートする必要があります。 ITL_Recovery 証明書をインポートするための新しいオプションが [一括証明書管理] の **証明書タイプ** ドロップダウンリストに追加されました。

証明書の一括エクスポートを使用するには、以下の手順を実行します。

手順

ステップ 1 [Cisco Unifiedオペレーティングシステムの管理(Cisco Unified Operating System Administration)] で、**[セキュリティ(Security)]** > **[証明書の管理]** の順に選択します。

ステップ 2 新しい宛先クラスタ (TFTP のみ) から中央の SFTP サーバに証明書をエクスポートします。

ステップ 3 一括証明書インターフェイスを使用して、SFTP サーバー上の証明書を統合する（TFTP のみ）。

ステップ 4 元のクラスターで一括証明書機能を使用して、中央の SFTP サーバから TFTP 証明書をインポートします。

ステップ 5 DHCP オプション 150 または他の方法を使用して、電話を新しい宛先クラスタにポイントします。

電話は新しい宛先クラスタ ITL ファイルをダウンロードし、既存の ITL ファイルに対して確認しようとします。 証明書が既存の ITL ファイルにないため、電話は古い TVS サーバに新しい ITL ファイルの署名を確認するよう要求します。 電話は、このリクエストを行うために、TCP ポート 2445 で TVS クエリを古い元のクラスターに送信します。

証明書のエクスポート/統合/インポートのプロセスが正しく機能する場合、TVS は成功を返し、電話はメモリ内の ITL ファイルを新しくダウンロードされた ITL ファイルで置き換えます。

電話は新しいクラスタから署名された構成ファイルをダウンロードし、確認できます。

証明書の表示

[証明書リスト] ページのフィルタ オプションを使用して、共通名、有効期限日付、キー タイプ、および使用方法に基づいて証明書のリストを並べ替えて表示できます。 このため、フィル

タオプションを使用すると、データの並べ替え、表示、およびデータの効率的な管理を行えます。

Unified Communications Manager リリース 14 から、使用オプションを選択して、ID または信頼証明書のリストを並べ替え、表示できます。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）][証明書の管理（Certificate Management）]** を選択します。
[Certificate List] ページが表示されます。

ステップ 2 **[証明書リストの検索場所]** ドロップダウンリストから、必要なフィルタオプションを選択し、**[検索]** フィールドに検索項目を入力して **[検索]** ボタンをクリックします。

たとえば、アイデンティティ証明書だけを表示するには、**[証明書の一覧の検索条件（Find Certificate List where）]** ドロップダウンリストから **[使用法（Usage）]** を選択し、**[検索（Find）]** フィールドにアイデンティティを入力して、**[検索（Find）]** ボタンをクリックします。

証明書のダウンロード

CSR リクエストを送信する際、ダウンロード証明書タスクを使用して証明書のコピーを作成するか、証明書をアップロードします。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 検索情報を指定し、**[検索（Find）]** をクリックします。

ステップ 3 必要なファイル名を選択し、**[ダウンロード]** をクリックします。

中間証明書のインストール

中間証明書をインストールするには、まずルート証明書をインストールしてから、署名付き証明書をアップロードする必要があります。 この手順は、認証局から 1 つの署名付き証明書と複数の証明書が証明書チェーンで提供されている場合にのみ必要です。

手順

ステップ 1 [Cisco Unified OS の管理（Cisco Unified OS Administration）] から、**[セキュリティ（Security）]**> **[証明書の管理（Certificate Management）]** をクリックします。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書の用途]** ドロップダウンリストで適切な信頼ストアを選択して、ルート証明書をインストールします。

ステップ 4 選択した証明書の説明を入力します。

ステップ 5 次のいずれかの手順を実行して、アップロードするファイルを選択します。

- [ファイルのアップロード（Upload File）]テキスト ボックスに、ファイルへのパスを入力します。
- [参照（Browse）]をクリックしてファイルに移動し、[開く（Open）]をクリックします。

ステップ 6 [アップロード（Upload）]をクリックします。

ステップ 7 顧客証明書をインストールしたら、FQDN を使用して Cisco Unified Intelligence Center の URL にアクセスします。 IP アドレスを使用して Cisco Unified Intelligence Center にアクセスすると、カスタム証明書を正常にインストールした後でも「ここをクリックしてログインを継続します（Click here to continue）」のメッセージが表示されます。

（注）

- TFTP Tomcat 証明書をアップロードするときは、TFTP サービスを再起動する必要があります。 それ以外の場合は、TFTP は古いキャッシュの自己署名された tomcat 証明書を提供し続けます。
- 電話機のエッジ信頼から証明書をアップロードするには、発行元から行う必要があります。

信頼証明書の削除

削除できる証明書は、信頼できる証明書だけです。 システムで生成される自己署名証明書は削除できません。

注意 証明書を削除すると、システムの動作に影響する場合があります。 また、証明書が既存のチェーンの一部である場合、証明書チェーンが壊れることがあります。 この関係は、**[証明書の一覧（Certificate List）]** ウィンドウ内の関連する証明書のユーザ名とサブジェクト名から確認します。 この操作は取り消すことができません。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 証明書の一覧をフィルタするには、**[検索（Find）]** コントロールを使用します。

ステップ 3 証明書のファイル名を選択します。

ステップ 4 [削除（Delete）]をクリックします。

ステップ 5 **OK**をクリックします。

（注）
- 削除する証明書が 「CAPF-trust」、「tomcat-trust」、「CallManager-trust」、または「Phone-SAST-trust」 証明書タイプの場合、証明書はクラスタ内のすべてのサーバで削除されます。
- 電話機のエッジトラストからの証明書の削除は、発行元から行う必要があります。
- 証明書をCAPF-trustにインポートする場合、それはその特定のノードでのみ有効になり、クラスタ全体で複製されることはありません。

証明書署名要求の生成

証明書署名要求（CSR）を生成します。これは、公開キー、組織名、共通名、地域、および国などの証明書申請情報を含む暗号化されたテキストのブロックです。 認証局はこの CSR を使用して、ご使用のシステムの信頼できる証明書を生成します。

（注） 新しい CSR を生成すると、既存の CSR は上書きされます。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 [CSR の作成（Generate CSR）]をクリックします。

ステップ 3 **[証明書署名要求の作成]** ウィンドウのフィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 4 [Generate]をクリックします。

証明書署名リクエストのフィールド

表 *9*: 証明書署名リクエストのフィールド

フィールド	説明
証明書の用途	ドロップダウンメニューから次の値を選択します。 • **CallManager** • **CallManager-ECDSA**

配布	Unified Communications Manager サーバを選択します。
	ECDSA のマルチサーバーにこのフィールドを選択するには、次の構文を使用します。
	`Callmanager-ecdsa common name: <host-name>-EC-ms.<domain>`
	RSA のマルチサーバーにこのフィールドを選択するには、次の構文を使用します。
	`Callmanager common name: <host-name>-ms.<domain>`

共通名/共通Name_SerialNumber	**重要** リリース 14SU1 以降でサポートされます。 共通名または共通名に証明書のシリアル番号を付加したものが表示されます。 共通名または共通Name_SerialNumber は証明書のファイル名です。 **配信** フィールドでデフォルトで選択した Unified Communications Manager アプリケーションの名前を表示します。
自動入力ドメイン	このフィールドは、[サブジェクト代替名(SAN)（Subject Alternate Names (SANs)）] セクションに表示されます。 1 つの証明書で保護されるホスト名が一覧で表示されます。
親ドメイン	このフィールドは、[サブジェクト代替名(SAN)（Subject Alternate Names (SANs)）] セクションに表示されます。 デフォルトドメイン名が表示されます。必要に応じて、ドメイン名を変更できます。
キータイプ	このフィールドで、公開秘密キーペアの暗号化および復号化に使用するキーのタイプを識別します。 Unified Communications Manager は、 **EC** および **RSA** 鍵タイプをサポートしています。

フィールド	説明
キーの長さ	**[キー長（Key Length）]** ドロップダウンメニューから、いずれかの値を選択します。 キー長に応じて、CSR リクエストのハッシュアルゴリズムの選択肢が制限されます。 ここでハッシュアルゴリズムの選択肢が制限されることで、キー長と同じかそれ以上の強度を持つハッシュアルゴリズムを使用できます。 たとえば、キー長が 256 の場合は、SHA256、SHA384、SHA512 からハッシュアルゴリズムを選択できます。 同様に、キー長が 384 の場合は、SHA384 または SHA512 からハッシュアルゴリズムを選択できます。 （注） RSA 証明書については、[Key Length] の値が 3072 または 4096 の証明書のみを選択できます。 これらのオプションは、ECDSA 証明書では使用できません。 （注） CallManager **[証明書の目的（Certificate Purpose）]** で選択された RSA **キーの長さ**が 2048 を超えると、電話機の機種によっては登録に失敗することがあります。Cisco Unified Reporting Tool（CURT）の Unified CM 電話機能リストレポートから、**3072/4096 RSA キーサイズサポート**機能でサポートされている電話モデルのリストを確認できます。
ハッシュ アルゴリズム（Hash Algorithm）	**[Hash Algorithm（ハッシュアルゴリズム）]** ドロップダウンメニューから値を選択して、ハッシュアルゴリズムの強度を楕円曲線のキー長よりも強くします。 **[Hash Algorithm（ハッシュアルゴリズム）]** ドロップダウンメニューから、いずれかの値を選択します。 （注） • **[Hash Algorithm（ハッシュアルゴリズム）]** の値が、**[キー長（Key Length）]** フィールドで選択した値に応じて変わります。 • システムが FIPS モードで稼働している場合は、ハッシュアルゴリズムに必ず SHA256 を選択してください。

証明書署名要求のダウンロード

CSR を作成後、ダウンロードして、認証局に証明書を送信できるようにします。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 [CSR のダウンロード（Download CSR）]をクリックします。

ステップ 3 [証明書の用途（Certificate Purpose）] ドロップダウン リストで、証明書名を選択します。

ステップ 4 [CSR のダウンロード（Download CSR）]をクリックします。

ステップ 5 （任意） プロンプトが表示されたら、[保存（Save）]をクリックします。

自己署名証明書の生成

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。
[証明書の一覧（Certificate List）]ウィンドウが表示されます。

ステップ 2 検索パラメータを入力して、証明書を検索して設定の詳細を表示します。
すべての条件に一致したレコードが **[Certificate List]** ウィンドウに表示されます。

ステップ 3 **[自己署名証明書の生成]** をクリックして新しい自己署名証明書を生成します。
[新しい自己署名証明書の生成] ウィンドウが表示されます。

ステップ 4 **証明書の目的** ドロップダウンボックスから、システムセキュリティ証明書を選択します (例: **CallManager-ECDSA**)。

ステップ 5 **[新しい自己署名証明書]** ウィンドウのフィールドを設定します。 フィールドとその設定オプションの詳細については、「関連項目」の項を参照してください。

ステップ 6 [Generate]をクリックします。

関連トピック

自己署名証明書のフィールド （56 ページ）

自己署名証明書のフィールド

表 *10 :* 自己署名証明書のフィールド

フィールド	説明
証明書の用途	ドロップダウンメニューから、必要なオプションを選択します。 次のいずれかのオプションを選択すると、**[キータイプ（Key Type）]** フィールドが自動的に **[RSA]** に設定されます。 • Cisco Tomcat • ipsec • ITL リカバリ • CallManager • CAPF • TVS 次のいずれかのオプションを選択すると、**[キータイプ（Key Type）]** フィールドが自動的に **[EC]**（楕円曲線）に設定されます。 • tomcat-ECDSA • CallManager-ECDSA
配布	ドロップダウン メニューから Unified Communications Manager サーバを選択します。
共通名/共通 Name_SerialNumber	共通名または共通名に証明書のシリアル番号を付加したものが表示されます。 共通名または共通Name_SerialNumberは証明書のファイル名です。

フィールド	説明
自動入力ドメイン	**[証明書の用途（Certificate Purpose）]** ドロップダウンメニューで次のいずれかのオプションを選択した場合にのみ表示されます。 • tomcat • tomcat-ECDSA • CallManager • CallManager-ECDSA • TVS このフィールドには、単一の証明書で保護されるホストの名前が一覧で表示されます。 証明書の共通名はホスト名と同じです。 **CallManager-ECDSA** と **tomcat-ECDSA** の両方の証明書に、ホスト名とは異なる共通名が付けられます。 このフィールドには、 **CallManager-ECDSA** 証明書の完全修飾ドメイン名が表示されます。
キータイプ	このフィールドには、公開秘密キーペアの暗号化および復号化に使用するキーのタイプが一覧で表示されます。 Unified Communications Manager は、 **EC** および **RSA** 鍵タイプをサポートしています。

フィールド	説明
キーの長さ	次のいずれかの値をドロップダウンメニューから選択します。 • 1024 • 2048 • 3072 • 4096 キー長に応じて、自己署名証明書リクエストのハッシュアルゴリズムの選択肢が制限されます。 ハッシュアルゴリズムの選択肢が制限されることで、キー長と同じかそれ以上の強度を持つハッシュアルゴリズムを使用できます。 • キー長の値が 256 の場合、SHA256、SHA384、SHA512 からハッシュアルゴリズムを選択できます。 • キー長の値が 384 の場合は、SHA384 または SHA512 からハッシュアルゴリズムを選択できます。 （注） **[キー長（[Key Length）]** の値に 3072 または 4096 を選択する証明書は RSA 証明書のみです。 これらのオプションは、ECDSA 証明書については使用できません。 （注） CallManager の **[証明書の用途（Certificate Purpose）]** で選択された RSA の **[キー長（key length）]** が 2048 を超えると、電話機のモデルによっては登録に失敗することがあります。 詳細については、Cisco Unified Reporting Tool（CURT）の **Unified CM 電話機能リストレポート**から、**33072/4096 RSA キーサイズサポート**機能でサポートされている電話モデルのリストをチェックしてください。
ハッシュアルゴリズム（Hash Algorithm）	ドロップダウンメニューから、キー長と同じかそれ以上の値を選択します。 （注） • **[ハッシュアルゴリズム（Hash Algorithm）]** ドロップダウンリストの値は、**[キー長（Key Length）]** フィールドで選択した値に応じて変わります。 • システムが FIPS モードで稼働している場合は、ハッシュアルゴリズムに必ず SHA256 を選択してください。

フィールド	説明
	ドロップダウンリストから5、10、20などのオプションのいずれかを選択して、自己署名証明書の有効期間を設定します。

証明書の再作成

有効期限が切れる前に証明書を再生成することをお勧めします。 RTMT（Syslog Viewer）で警告が発行され、証明書の期限が近くなると電子メールで通知が送信されます。

ただし、期限切れの証明書を再生成することもできます。電話機を再起動してサービスを再起動する必要があるため、営業時間後にこのタスクを実行します。 Cisco Unified OS の管理に「cert」タイプとしてリストされている証明書のみ再作成できます。

⚠

注意 証明書を再生成すると、システムの動作に影響する場合があります。証明書を再作成すると、サードパーティの署名付き証明書（アップロードされている場合）を含む既存の証明書が上書きされます。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

検索パラメータを入力して、証明書を検索して設定の詳細を表示します。すべての条件に一致したレコードが [**Certificate List**] ウィンドウに表示されます。

証明書の詳細ページで**[再生成（Regenerate）]**ボタンをクリックすると、同じキー長を持つ自己署名証明書が再生成されます。

（注）
証明書を再生成した場合、**[再生成（Regeneration）]** ウィンドウを閉じて、新しく生成された証明書を開くまで、**[証明書の説明（Certificate Description）]** フィールドは更新されません。

3072または4096の新しいキー長の自己署名証明書を再生成するには、[**自己署名証明書の生成（Generate Self-Signed Certificate**）] をクリックします。

ステップ 2 [**自己署名証明書の新規作成（Generate New Self-Signed Certificate**）] ウィンドウのフィールドを設定します。 フィールドおよびその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 3 [Generate]をクリックします。

ステップ 4 再作成された証明書の影響を受けるサービスをすべて再起動します。

ステップ 5 CAPF、ITLRecovery証明書またはCallManager証明書の再生成後にCTLファイルを更新します（設定している場合）。

（注）

証明書を再作成したら、システムのバックアップを実行して、最新のバックアップに再作成した証明書が含まれるようにします。バックアップに再作成した証明書が含まれていない状態でシステムの復元タスクを実行する場合は、システム内の各電話機のロックを手動で解除して、電話機を登録できるようにする必要があります。

重要
CallManager、CAPF、および TVS 証明書が再生成または更新されると、電話機は自動的にリセットされ、更新された ITL ファイルを受信します。

証明書の名前と説明

次の表に、再作成可能なシステムのセキュリティ証明書と、再起動する必要がある関連サービスを示します。 TFTP 証明書の再作成の詳細については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html の『*Cisco Unified Communications Manager* セキュリティガイド』を参照してください。

表 *11* : 証明書の名前と説明

Name	Description	再起動が必要なサービス
tomcat tomcat-ECDSA	この証明書は、SIP Oauth モードが有効になっているときに Web サービス、Cisco DRF サービス、および Cisco CallManager サービスで使用されます。	Cisco Tomcat サービス、Cisco CallManager サービス。
ipsec	この自己署名ルート証明書は、Unified Communications Manager、MGCP、H.323、IM and Presence Service との IPsec 接続のインストール中に生成されます。	CLI から **utils ipsec restart** コマンドを使用して IPSec サービスを再起動できます。
CallManager CallManager-ECDSA	これは SIP、SIP トランク、SCCP、TFTP などに使用されます。	Cisco Call Manager サービスおよびその他の関連サービス（Cisco CTI Manager を含む）- サーバーがセキュアモードの場合、CTL ファイルを更新します。 CallManager-ECDSA - Cisco CallManager サービス。

Name	Description	再起動が必要なサービス
CAPF	Unified Communications Manager Publisher ノードで実行されている CAPF サービスによって使用されます。 この証明書は、エンドポイントに LSC を発行するために使用されます(オンラインおよびオフライン CAPF モードを除く)。	クラスタ ノードで SIP OAuth が有効になっている場合は、Cisco HAProxy を再起動します。
TVS	これは Trust 検証サービスで使用されます。これは、サーバ証明書が変更された場合に電話機のセカンダリ信頼検証メカニズムとして機能します。	該当なし
ITL リカバリ	この証明書は、ITL ファイルと CTL ファイルの両方に署名します。SAML SSO アサーションの署名にも使用されます。	証明書が再生成されるたびに、サービスは自動的に再起動されます。 Tomcat 証明書で SAML SSO が有効になっている場合は、IDP で SP メタデータを再プロビジョニングする必要があります。

重要 この注意事項は、リリース 14SU2 にのみ適用されます。

リリース 14SU2 では、tomcat-ECDSA 証明書の再生成またはアップロードの後に Cisco DRF サービスを再起動する必要があります。 tomcat RSA 証明書の処理後に再起動する必要はありません。

CAPF 証明書の再生成

CAPF 証明書を再生成するには、以下の手順を実行します。

(注) CAPF 証明書がパブリッシャにある場合、電話が ITL ファイルを更新するために自動的に再起動するのを確認できます。 この動作は、証明書更新時の電話によるやり取りパラメータが自動的にリセットされた場合に適用されます。

手順

ステップ 1 CAPF 証明書を再生成します。

ステップ 2 CTL ファイルがある場合は、CTL ファイルを更新する必要があります。

詳細については、証明書の再作成 （59 ページ） を参照してください。

ステップ 3 CAPF 証明書が再生成されると、CAPF サービスが自動的に再起動されます。

『*Cisco Unified Communications Manager* セキュリティガイド』にある「「認証局プロキシ機能サービスを有効にする」」の項を参照してください。

TVS 証明書の再生成

（注） TVS および TFTP 証明書の再生成を計画している場合、TVS 証明書を再生成し、電話の再起動が完了するのを待ってから、TFTP 証明書を再生成します。 これは、[証明書更新時の電話との対話] パラメーターが自動的にリセットされる場合に適用されます。

手順

TVS 証明書を再生成します。

詳細については、『Cisco Unified Communications Manager セキュリティ ガイド』の「証明書の再生成」セクションを参照してください。

CTL ファイルには TVS 証明書が含まれていません。 したがって、TVS 証明書が再生成される場合は、CTL ファイルを更新する必要はありません。

TVS 証明書が再生成されると、TVS サービスは自動的に再起動されます。

CallManager 証明書の再生成

CallManager 証明書を再生成するには、次の手順に従います。

（注） 複数の証明書を再生成する予定の場合は、最後に TFTP 証明書を再生成する必要があります。 電話の再起動が完了するのを待ってから、TFTP 証明書を再生成してください。 この手順を実施しない場合、すべての Cisco IP 電話から ITL ファイルを手動で削除する必要があります。 このルールは、Phone interaction on Certificate Update パラメータが自動的にリセットされる場合に適用されます。

手順

ステップ 1 CallManager 証明書を再生成します。

詳細については、『Cisco Unified Communications Manager 管理ガイド』を参照してください。

ステップ 2 TFTP サービスが有効になっている場合は、すべての電話が自動的に再起動するまで待ちます。

ステップ 3 クラスターが混合モードの場合、CTL ファイルを更新します。

ステップ 4 クラスターが EMCC 展開の一部である場合、一括証明書プロビジョニングの手順を繰り返します。

詳細については、『Cisco Unified Communications Manager 管理ガイド』を参照してください。

TFTP 証明書の再生成後のシステムバックアップ手順

ITL ファイルのトラストアンカーはソフトウェア エンティティである TFTP 秘密鍵です。 サーバがクラッシュした場合、キーが失われ、電話は新しい ITL ファイルを検証できなくなります。

Unified Communications Manager リリース 10.0 では、TFTP 証明書と秘密鍵の両方が災害復旧システムによりバックアップされます。 システムはバックアップパッケージを暗号化して、秘密鍵を秘密に保つ。 サーバがクラッシュした場合、以前の証明書とキーが復元されます。

TFTP 証明書が再生成されるたびに、新しいシステムバックアップを作成する必要があります。バックアップ手順については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。

ITLRecovery 証明書の再生成

警告 ITLRecovery 証明書は頻繁に再生成しないでください。この証明書には電話で長い有効期間があり、CallManager 証明書が含まれているためです。

非セキュア クラスタの ITLRecovery 証明書を再生成する

1. ITL ファイルが有効かどうか、およびクラスタ内のすべての電話が現在の ITL ファイルを信頼していることを確認してください。
2. ITLRecovery 証明書を再生成します。

   各クラスタのパブリッシャに移動して、ITLRecovery 証明書を再生成します。

   1. [Cisco Unified OS Administration] から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。
   2. **[検索（Find）]** をクリックします。

[証明書の一覧（Certificate List）] ウィンドウが表示されます。

3. 表示される証明書のリストから、[ITLRecovery.pem Certificate] リンクをクリックします。
4. [**再生成**] をクリックして、ITLRecovery 証明書を再生成します。
5. 確認メッセージのポップアップで、[**OK**] をクリックします。

3. ITLファイルに署名するために `utils itl reset localkey` をCallManager証明書で使用し、新しい ITL ファイルを受け入れます。
4. クラスタ内のすべての電話をバッチでリセットします。

（注） クラスタ内のすべての電話が登録されていることを確認してください。

5. 新しい ITLRecovery 証明書で ITL ファイルに再署名するために、TFTP サービスを再起動します。

   電話がリセットされると、新しい ITLRecovery 証明書が電話にアップロードします。
6. 新しい ITL ファイルを取得するために、クラスタ内のすべての電話を 2 回目にバッチでリセットします。
7. 電話機はリセット後に新しい ITLRecovery 証明書で更新されます。

セキュア クラスタの ITLRecovery 証明書を再生成する

トークン ベースの ITL ファイルからトークンレス ITL ファイルに移行する場合は、セキュリティ ガイドの移行セクションを参照してください。

1. ITL ファイルが有効かどうか、およびクラスタ内のすべての電話が現在の ITL ファイルを信頼していることを確認してください。
2. `show ctl` コマンドを使用して CTL ファイルを確認してください。
3. ITLRecovery 証明書を再生成してください。

   各クラスタのパブリッシャに移動して、ITLRecovery 証明書を再生成してください。

   1. [Cisco Unified OS Administration] から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）] > [検索（Find）]** を選択します。
   2. 証明書の一覧を検索するには、[**検索**] をクリックします。

      [証明書の一覧（Certificate List）] ウィンドウが表示されます。
   3. 表示される証明書のリストから、[ITLRecovery.pem 証明書] リンクをクリックします。
   4. [**再生成**] をクリックして、ITLRecovery 証明書を再生成します。
   5. 確認メッセージのポップアップで、[**OK**] をクリックします。

4. CallManager 証明書で `utils ctl reset localkey` を使用して CTLFile に署名します。 これにより、新しい ITLRecovery 証明書で CTLFile も更新されます。
5. クラスター内のすべての電話をバッチでリセットして、新しい ITLRecovery 証明書を持つ新しい CTLFile を選択します。

（注）
- クラスタ内のすべての電話が登録されていることを確認してください。
- システム全体の証明書が有効化に使用される場合、ITLRecovery の再生成はクラスタの SAML SSO ログインに影響を与えます。

6. 新しい ITLRecovery Certificate で再署名するために CTLFile を更新します `utils ctl update CTLFile`。
7. クラスター内のすべての電話を再度バッチでリセットし、新しい ITLRecovery 証明書によって署名された新しい CTLFile をピックアップします。
8. 電話機はリセット後に新しい ITLRecovery 証明書で更新されます。

Tomcat 証明書の再生成

（注） SIP OAuth が有効な場合、Tomcat 証明書の再生成とサービスの再起動後に、Cisco CallManager サービスを再起動する必要があります。

Tomcat 証明書を再生成するには、以下の手順を実行します。

手順

ステップ 1 Tomcat 証明書を再生成します。

詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。

ステップ 2 Tomcat サービスの再起動

詳細については、 *Cisco Unified Communications* 管理者ガイドを参照してください。

ステップ 3 クラスターが EMCC 展開の一部である場合、一括証明書プロビジョニングの手順を繰り返してください。

詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。

OAuth 更新ログイン用のキーの再生成

コマンドラインインターフェイスを使用して暗号キーと署名キーの両方を再生成するには、この手順を使用します。 Cisco Jabber が Unified Communications Manager との OAuth 認証に使用する暗号キーまたは署名キーが侵害された場合にのみ、この作業を実行します。 署名キーは非対称で RSA ベースであるのに対し、暗号キーは対称キーです。

このタスクを完了すると、これらのキーを使用する現在のアクセストークンと更新トークンは無効になります。

エンドユーザへの影響を最小限に抑えるために、このタスクは営業時間外に完了することを推奨します。

暗号キーは、以下の CLI を使用してのみ再生成できますが、発行元の Cisco Unified OS の管理 GUI を使用して署名キーを再生成することもできます。 **[セキュリティ]** > **[証明書の管理]** を選択し、**AUTHZ** 証明書を選択して、**[再作成]** をクリックします。

手順

ステップ 1 Unified Communications Manager発行元ノードで**コマンドライン**インターフェイスにログインします。

ステップ 2 暗号キーを再生成するには、次の手順を実行します。

a) `set key regen authz encryption` コマンドを実行します。
b) 「`yes`」と入力します。

ステップ 3 署名キーを再生成するには、次の手順を実行します。

a) `set key regen authz signing` コマンドを実行します。
b) 「`yes`」と入力します。
Unified Communications Manager パブリッシャ ノードがキーを再生成し、IM and Presence Service のローカルノードを含めたすべての Unified Communications Manager クラスタノードに新しいキーを複製します。

すべての UC クラスタで新しいキーを再生成して同期する必要があります。

- IM and Presence 中央クラスタ：IM and Presence 集中型展開の場合、IM and Presence ノードはテレフォニーとは別のクラスタ上で実行されています。 この場合、IM and Presence Service の中央クラスタの Unified Communications Manager パブリッシャ ノードで、この手順を繰り返します。
- Cisco Expressway または Cisco Unity Connection：これらのクラスタ上でもキーを再生成します。 詳細については、Cisco Expressway および Cisco Unity Connection のマニュアルを参照してください。

（注）

キーを再割り当てした後、クラスタ内のすべてのノードでCisco CallManagerサービスを再起動します。

信頼ストアへの認証局署名済み CAPF ルート証明書の追加

認証局が署名した CAPF 証明書を使用する場合は、ルート証明書をUnified Communications Manager信頼ストアに追加します。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書/証明書チェーンのアップロード]** ポップアップ ウィンドウで、**[証明書の用途]** ドロップダウン リストから **[CallManager の信頼性]** を選択し、認証局署名済み CAPF ルート証明書を参照します。

ステップ 4 **[ファイルのアップロード]** フィールドに証明書が表示されたら、**[アップロード]** をクリックします。

CTL ファイルの更新

この手順を使用して、CLI コマンド経由で CTL ファイルを更新します。 混合モードが有効になっている場合、新しい証明書をアップロードするたびに CTL ファイルを更新する必要があります。

手順

ステップ 1 Unified Communications Manager パブリッシャノードから、 **コマンドラインインターフェース** にログインします。

ステップ 2 `utils ctl update CTLFile` コマンドを実行します。 CTL ファイルが再生成されると、ファイルは TFTP サーバにアップロードされ、電話に自動的に送信されます。

連携動作と制限事項

- **TLS_ECDHE_ECDSA_WITH_AES256_SHA384** および **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** に対応していないSIPデバイスでも、**TLS_ECDHE_RSA_WITH_AES_256_SHA384**、**TLS_ECDHE_RSA_WITH_AES_128_SHA256**、または **AES128_SHA**で接続することがで

きます。 これらのオプションは、選択した TLS 暗号オプションによって異なります。 [**ECDSA のみ**] オプションを選択すると、ECDSA 暗号をサポートしない端末は SIP インターフェイスへの TLS 接続を確立できなくなります。 **[ECDSA のみ（ECDSA only）]** オプションを選択した場合、このパラメータの値は **TLS_ECDHE_ECDSA_WITH_AES128_SHA256** および **TLS_ECDHE_ECDSA_WITH_AES256_SHA384**です。

- CTI マネージャセキュアクライアントは **TLS_ECDHE_RSA_WITH_AES_128_SHA256**、**TLS_ECDHE_RSA_WITH_AES_256_SHA384**、**TLS_ECDHE_ECDSA_WITH_AES_128_SHA256**、および **TLS_ECDHE_ECDSA_WITH_AES_256_SHA384** をサポートしていません。 しかし、**AES128_SHA** での接続は可能です。
- Unified Communications Manager は、同じ SubjectDN を持つ複数の証明書が同じ信頼ストアにアップロードされることをサポートしていません。 サーバーで新規と既存の証明書を区別するため、ユーザーには、異なる名前の新しいCN を使用するか、SubjectDN-issue-CA-G2 または SubjectDN-issue-CA-2023 のような文字をサフィックスとして使用することを推奨します。 それに対してハッシュリンクが作成されます。

証明書の監視と失効

このセクションでは、更新が必要な証明書を監視し、期限切れの証明書を失効させることができます。

証明書の監視の概要

Unified Communications Manager および IM and Presence Service サービスに自動システムが含まれるとき、管理者は証明書を追跡して更新できる必要があります。証明書の監視は、管理者が継続的に証明書の状況を把握し、証明書の有効期限が近づいたらメールで通知するのに役立ちます。

証明書モニタの設定(Certificate Monitor Configuration)

[Cisco Certificate Expiry Monitor] ネットワーク サービスを実行している必要があります。デフォルトでこのサービスは有効化されていますが、**[ツール（Tools）]** > **[コントロール センター - ネットワーク サービス（Control Center - Network Services）]** を選択し、[Cisco Certificate Expiry Monitor サービス（Cisco Certificate Expiry Monitor Service）] の状態が [実行中（Running）] であることを検証して Cisco Unified Serviceability でサービスが実行中であることを確認できます。

手順

ステップ 1 Cisco Unified OS 管理で **セキュリティ** > **Certificate Monitor を選択します**

ステップ 2 構成の詳細を入力または選択します。

ステップ 3 [Save]をクリックして、設定を保存します。

（注）
既定では、証明書監視サービスは 24 時間に 1 回実行されます。 証明書モニタ サービスを再起動すると、サービスが開始され、24 時間後に実行する次のスケジュールが計算されます。 証明書の有効期限日の 7 日間が近づいている場合でも、間隔は変更されません。 証明書の有効期限が切れた場合、または 1 日後に期限切れになる場合に、1 時間ごとに実行されます。

証明書失効の概要

この項では、証明書の失効について理解することができます。 Cisco UCM は、証明書失効を監視するための Online Certificate Status Protocol (OCSP) をプロビジョニングします。 証明書がアップロードされ、定期的なタイミングで、システムはステータスをチェックして有効性を確認します。

共通基準モードが有効な FIPS 展開の場合、OCSP はシステムが共通基準要件に準拠するように支援します。

証明書失効の設定

Unified Communications Manager 証明書のステータスをチェックし、有効性を確認します。

証明書の検証手順は以下の通りです。

- Unified Communications Manager Delegated Trust Model (DTM) を使用し、ルート CA または中間 CA の OCSP 署名属性を確認します。 ルート CA または中間 CA は、ステータスを確認するために OCSP 証明書に署名する必要があります。
- 委任された信頼モデルが失敗した場合、信頼レスポンダーモデル (TRP) にフォールバックします。 Unified Communications Manager は、OCSP サーバからの指定 OCSP 応答署名証明書を使用して、証明書を検証します。

（注） 証明書の失効ステータスを確認するために、OCSP レスポンダが実行されている必要があります。

システムが期限切れの証明書を自動的に失効させるように、OCSP を設定します。 証明書失効ウィンドウで OCSP オプションを有効にして、証明書失効をリアルタイムで安全に確認する手段を提供します。 証明書の OCSP URI を使用するか、構成された OCSP URI を使用するかオプションから選択します。

（注） syslog、FileBeat、SIP、ILS、LBM などの TLS クライアントは、OCSP からリアルタイムで失効応答を受信します。

システムにOCSPチェックに必要な証明書があることを確認してください。 OCSP応答属性で設定されたルートまたは中間CA証明書、またはtomcat-trustにアップロードされた指定されたOCSP署名証明書を使用できます。

手順

ステップ1 Cisco Unified OS Administration で、**[セキュリティ（Security）]** > **[証明書失効（Certificate Revocation）]** を選択します。

ステップ2 **[OCSP 有効化]** チェックボックスをオンにします。

ステップ3 証明書が OCSP レスポンダ URI で設定されている場合、[**証明書の OCSP URI を使用**] オプションをクリックします。

または

ステップ4 OCSP チェックに OCSP レスポンダを指定する場合は、[**設定済みの OCSP URI** を使用] オプションをクリックします。

ステップ5 レスポンダの **OCSP 設定済み URI** を入力します。

ステップ6 [**失効確認を有効にする**] チェックボックスにチェックを入れ、失効確認を有効にします。

ステップ7 失効ステータスを確認する **頻度** を入力して、[時間] または [日] から[ ]の間隔をクリックします。

ステップ8 **[保存（Save）]** をクリックします。

（注）
ポップアップが表示され、Cisco サービスのリストを再起動してリアルタイム OCSP を有効にするように警告されます。 このポップアップは、[**OCSP を有効にする**] にチェックを入れるか、その後の変更を保存した場合にのみ表示されます。

OCSP レスポンダは、検証と Common Criteria モードがオンの場合に、次のいずれかのステータスを返します。

- **正常** は、OCSP レスポンダーが状況の問い合わせに対して肯定的な応答を送信したことを示します。 証明書が失効していないということは、証明書が発行されたことや応答時間が証明書の有効期間内であることを必ずしも意味しません。 応答の拡張機能は、発行、有効性など、証明書のステータスに関して応答側によって提出されたより多くの主張を伝えます。
- **失効** 証明書が永久的または一時的に失効 (保留中) の状況であることを示します。
- **不明** は、OCSP レスポンダーが要求された証明書を知らないことを示します。

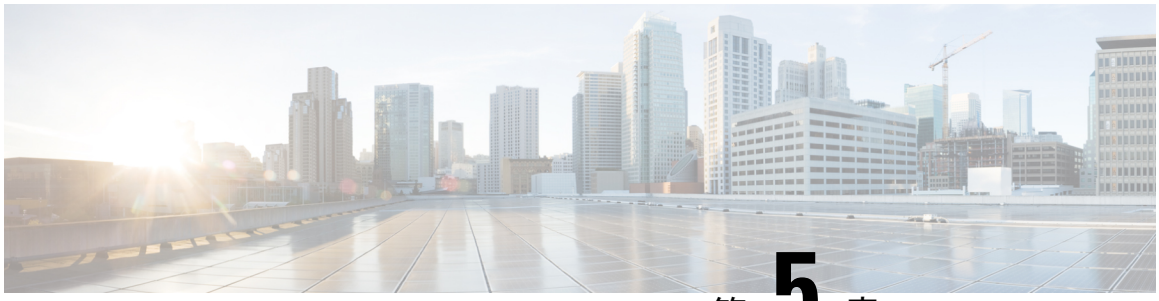
警告
共通基準モードを有効にすると、 **失効** および **不明** の場合に接続が失敗します。 コモンクライテリアモードを無効にすると、(**不明なケース**)接続に成功します。

ステップ9 （任意） CTI、IPsec または LDAP リンクがある場合は、これらの長期性接続の OCSP 失効サポートを有効にするために、上記の手順に加えて次の手順も行う必要があります。

a) Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。
b) [**証明書の失効と期限切れ**] ペインに移動します。
c) **パラメータ** 証明書の有効性チェックを **有効に設定してください**。
d) パラメータ **有効性チェック頻度** に値を入力してください。

（注）
[証明書失効] ウィンドウの **[失効チェックを有効にする（Enable Revocation Check）]** パラメータの間隔値は、**[有効チェック頻度（Validity Check Frequency）]** エンタープライズパラメータの値よりも優先されます。

e) **[保存（Save）]** をクリックします。



第 5 章

セキュリティモード

- セキュリティモードの概要 （73 ページ）
- 非セキュア モード (デフォルト モード) （73 ページ）
- セキュア モードの設定 （73 ページ）

セキュリティモードの概要

データや情報の改ざんを防ぐためのセキュリティメカニズムを実装するために、Unified Communications Manager は次のセキュリティモードを提供します。

- 非セキュア モード—デフォルト モード
- セキュア モードまたは混合モード - セキュアおよび非セキュア エンドポイントをサポートします。
- SIP 認証モード — セキュアな環境での Cisco Jabber 認証に OAuth 更新トークンを使用します

非セキュア モード (デフォルト モード)

初めてインストールするときの既定のセキュリティモードは、非セキュアモードです。 Unified Communications Manager このモードでは、 Unified Communications Manager はセキュアなシグナリングまたはメディアサービスを提供しません。

セキュア モードの設定

セキュリティを適用するには、展開に適用されるセキュリティモードを構成します。

手順

	コマンドまたはアクション	目的
ステップ 1	混合モード	混合モードを有効にすると、Cisco IP 電話と Webex デバイスのセキュリティが強化されます。 混合モードを有効にして確認する方法に関する情報を提供します。
ステップ 2	SIP OAuth モード	SIP OAuth モードを設定して、Cisco Jabber クライアントとその他のデバイスのセキュリティを強化します。

混合モード

混合モードまたはセキュア モードは、セキュアおよび非セキュア エンドポイントをサポートします。 クラスタまたはサーバに新たに Unified Communications Manager インストールすると、デフォルトで非セキュアモードになります。 ただし、セキュリティモードを非セキュアからセキュアまたは混合モードに変換することはできます。

クラスタを非セキュアモードから混合モード(セキュアモード)に変更するには、以下を実行します:

- 発行元で認証局プロキシ機能 (CAPF) サービスを有効にします。
- 発行元で証明書信頼リスト (CTL) サービスを有効にします。

Call Manager 証明書が自己署名の場合、CTL ファイルには各サーバのサーバ証明書、公開キー、シリアル番号、署名、発行者名、サブジェクト名、サーバ機能、DNS 名、および IP アドレスが含まれます。

Multi-SAN Call Manager 証明書の場合、CTL ファイルにはパブリッシャーの Call Manager 証明書が含まれています。

次に電話が初期化されるときに、TFTP サーバから CTL ファイルがダウンロードされます。 CTL ファイルに、自己署名証明書を持つ TFTP サーバエントリが含まれている場合、電話機は .sgn 形式の署名付き設定ファイルを要求します。 TFTP サーバに証明書が含まれていない場合、電話機は署名されていないファイルを要求します。

次のコマンドを実行して CTL ファイルを更新できます。

- **utils ctl set-cluster 混合モード**

  CTL ファイルを更新し、クラスタを混合モードに設定します。

- **utils ctl set-cluster ノンセキュア モード**

  CTL ファイルを更新し、クラスタをノンセキュア モードに設定します。

- **utils ctl update CTLFile**

  クラスターの各ノードで CTL ファイルを更新します。

（注） エンドポイントセキュリティでは、Transport Layer Security (TLS) がシグナリングに使用され、セキュアな RTP (SRTP) がメディアに使用されます。

混合モードを有効にするには、パブリッシャノードのコマンドラインインターフェースにログインし、CLI コマンド `utils ctl set-cluster 混合-モード`を実行します。

（注） Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されていることを確認してください。 スマートアカウントまたはバーチャルアカウントから受け取った登録トークンは、このクラスターに登録する際に、[輸出規制による機能限定の許可（Allow export-controlled functionality）] が有効になっています。

トークンレス CTL ファイルの場合、管理者は、Unified Communications Manager リリース 12.0(1) 以降で、USB トークンを使用して生成され、アップロードされた CTL ファイルをエンドポイントがダウンロードするようにする必要があります。 ダウンロード後、トークンレス CTL ファイルに切り替えることができます。 その後、util ctl update CLI コマンドを実行できます。

セキュリティモードを非セキュアからセキュアまたは混合モードに変更した場合、セキュリティモードを確認できます。 モードを確認するには、[**エンタープライズパラメータ設定**] ページに移動して、クラスタまたはサーバが混在モードになっていないことを確認してください。 詳細については、「セキュリティモードを確認する」トピックを参照してください。

セキュリティモードの確認

セキュリティモードを非セキュアからセキュアまたは混合モードに変更した場合、セキュリティモードを確認できます。 モードを確認するには、[**エンタープライズパラメータ設定**] ページに移動して、クラスタまたはサーバが混在モードかどうかを確認してください。

セキュリティモードを確認するには、以下の手順を実行します。

手順

ステップ 1 Unified Communications Manager Administration から **[システム]** > **エンタープライズパラメータ** を選択します。
[**エンタープライズパラメータの設定**] ページが表示されます。

ステップ 2 [**セキュリティパラメータ**] ペインに移動します。
[クラスターセキュリティモード（Cluster Security Mode）] フィールドが適切な値で見つかります。 値が 1 と表示されたら、Unified Communications Manager を混合モードに設定すること

に成功しています。 この値は Cisco Unified CM Administration Administration ページでは設定できません。 この値は、CLI コマンド `set utils cli` を入力した後に表示されます。

（注）
クラスタセキュリティモードは、スタンドアロンサーバまたはクラスタのセキュリティ機能を設定します。

SASTのCTLファイルの役割

（注） *次の表に記載されている署名者は、CTL ファイルへの署名に使用されます。

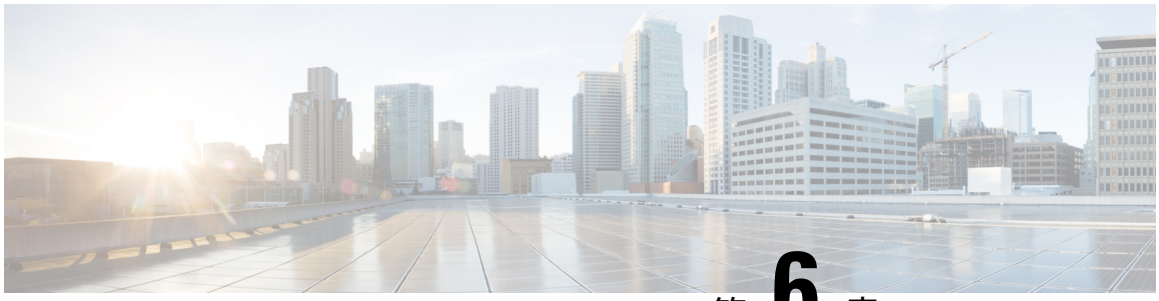
表 *12 :* システム管理者セキュリティトークン（*SAST*）の*CTL*ファイルの役割

Cisco Unified Communications Manager のバージョン	トークンベースのCTLファイルのシステム管理者セキュリティトークン（SAST）の役割	トークンレスのCTLファイルのシステム管理者セキュリティトークン（SAST）の役割
12.0(1)	トークン 1 (署名者*) トークン 2 ITL リカバリ CallManager	ITLRecovery (署名者) CallManager
11.5(x)	トークン 1 (署名者) トークン 2 ITL リカバリ CallManager	CallManager (署名者) ITL リカバリ
10.5(2)	トークン 1 (署名者) トークン 2	CallManager (署名者) ITL リカバリ
10.5(1) (サポートされていません)	トークン 1 (署名者) トークン 2	CallManager (署名者)
10.0(1) (サポートされていません)	トークン 1 (署名者) トークン 2	CallManager (署名者)
9.1(2)	トークン 1 (署名者) トークン 2	なし

SIP OAuth モード

SIP OAuth モードでは、セキュアな環境での Cisco Jabber 認証に OAuth 更新トークンを使用できます。 Unified Communications Manager の SIP 回線で OAuth をサポートすることで、CAPF なしでセキュアシグナリングとセキュアメディアが可能になります。 Unified Communication Manager クラスタおよび Cisco Jabber エンドポイントで OAuth ベースの認証を有効にすると、SIP 登録中の OAuth トークン検証が完了します。

SIP 登録に対する OAuth サポートは、Cisco Unified Communications Manager 12.5 (1) リリース以降の Cisco Jabber デバイスでのみ拡張されています。SIP OAuth の詳細は、 Cisco Unified Communications Manager 機能設定ガイドを参照してください。



第 6 章

暗号管理

- 暗号管理 （79 ページ）
- 暗号文字列の設定 （82 ページ）
- 暗号の制限 （85 ページ）
- 暗号の制限 （93 ページ）

暗号管理

暗号管理は、すべての TLS および SSH 接続で許可されるセキュリティ暗号のセットを管理できるオプション機能です。 暗号管理により、強度の低い暗号を無効にして、最小限のセキュリティレベルを有効にすることができます。

[**暗号管理**] ページにデフォルト値がありません。 代わりに、暗号管理機能は許可された暗号を設定した場合にのみ有効になります。 特定の脆弱な暗号は、[**暗号管理**] ページで設定されている場合でも、使用できません。

次の TLS および SSH インターフェイスで暗号を設定できます。

- **すべての TLS（All TLS）** ：このフィールドで指定される指定された暗号は、Unified Communications Manager および IM and Presence Serviceで TLS プロトコルをサポートするすべてのサーバーとクライアント接続に適用されます。
- **HTTPS TLS**：このフィールドで指定される暗号は、Unified Communications Manager と IM and Presence Service で TLS プロトコルをサポートするポート 443 および 8443 のすべての Cisco Tomcat 接続に適用されます。

（注） **[HTTPS TLS]** および **[すべての TLS（All TLS）]** フィールドに暗号を指定すると、**[HTTPS TLS]** によって**[すべての TLS（All TLS）]** の暗号が上書きされます。

- **SIP TLS**—このフィールドで指定される暗号は、Unified Communications Manager で TLS プロトコルをサポートする SIP TLS インターフェイスとの間のすべての暗号化接続に適用されます。 SCCP または CTI デバイスには適用されません。

認証済みモードの SIP インターフェイスは、NULL-SHA 暗号のみをサポートします。

SIP インターフェイスまたはすべてのインターフェイスで暗号を設定すると、認証モードはサポートされなくなります。

[SIP TLS] および **[すべての TLS（All TLS）]** フィールドに暗号を指定すると、SIP TLS で設定した暗号がすべての TLS 暗号を上書きします。

- **SSH 暗号**—このフィールドで指定された暗号は、 Unified Communications Manager および IM and Presence Serviceの SSH 接続に適用されます。
- **SSH 鍵交換**—このフィールドで指定された鍵交換アルゴリズムは、 Unified Communications Manager および IM and Presence Serviceの SSH インターフェースに適用されます。

曲線ネゴシエーション

以下は、曲線をネゴシエートするためのポイントです。

- ECDSA 暗号は、ECDSA 証明書のキーサイズに基づいて、異なる EC 曲線と自動的に選択されます。
- RSA 暗号は、証明書のキーサイズに関係なく、すべての EC 曲線と自動的に選択されます。
- TLS 自動選択を行うには、ECDSA 証明書のキーサイズが曲線サイズと同じである必要があります。

例：

クライアントが P-384 EC 曲線を提供すると、384 キー証明書と ECDSA 暗号が交渉されます。

曲線交渉は、RSA および ECDSA 暗号の両方に対するクライアントの優先度に基づいています。

証明書のサイズが 384 ビットで、クライアントに提供されるものが P-521、P-384、P-256 EC 曲線の場合、TLS 交渉は P-521 曲線で行われます。 クライアントが提供する曲線は最初は P-521 で、P-384 曲線もリストで利用可能です。 証明書のサイズが 384 ビットで、クライアントに提供されるものが P-521、P-256 EC 曲線である場合、クライアントは P-384 曲線を提供しないため、TLS ネゴシエーションは行われません。

以下は、EC 曲線でサポートされている暗号です。

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

```
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
```

推奨される暗号

デフォルトでは、Unified Communications Manager と IM and Presence Service はすでに一連の暗号（下記の「TLS および SSH 暗号」の項を参照）を使用し、サードパーティ製品を含む他のほとんどの製品とのセキュアな統合をサポートしています。したがって、変更する必要はありません。暗号スイートの不一致によって TLS ハンドシェイクが失敗する場合、Unified Communications Manager の暗号管理を使用して、サポートされている暗号のリストに追加の暗号を追加できます。

暗号管理は、顧客の制限を厳しくし、TLS ハンドシェイク中に特定の暗号スイートがネゴシエートされるのを防ぐ場合にも使用できます。暗号を設定した後で変更を有効にするには、影響を受けるサービスを再起動するか、サーバーをリブートします。

警告 SSH MAC インターフェイスで hmac-sha2-512 を設定すると、DRS および CDR 機能に影響します。

暗号 aes128-gcm@openssh.com の設定、"ssh Cipher の" フィールド内の aes256-gcm@openssh.com、または ssh kex "の sha2-nistp256 アルゴリズムのみを設定すると、DRS と CDR の機能が失われます。

CDR、AXL、DRS、および Bulk Certificate Exchange インターフェイスは、rsa-sha2-512 が設定されている場合でも、rsa-sha2-256 ホストキー アルゴリズムを使用します。

Cisco は、TLS および SSH インターフェイスの構成用に次の暗号ストリングをサポートしています。

TLS

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:
ECDHE-RSA-AES256-SHA:AES256-GCM-SHA384:AES256-SHA256:AES256-SHA:
ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-SHA256:
ECDHE-RSA-AES128-SHA:AES128-GCM-SHA256:AES128-SHA256:AES128-SHA
```

SSH 暗号

```
aes128-ctr,aes192-ctr,aes256-ctr,aes128-gcm@openssh.com,
aes256-gcm@openssh.com
```

SSH MAC

```
hmac-sha2-512,hmac-sha2-256,hmac-sha1
```

SSH KEX

```
ecdh-sha2-nistp521, ecdh-sha2-nistp384, ecdh-sha2-nistp256,
diffie-hellman-group14-sha1, diffie-hellman-group16-sha512,
diffie-hellman-group14-sha256
```

暗号文字列の設定

- **[すべての TLS（All TLS）]**、**[SIP TLS]**、および **[HTTPS TLS]** フィールドに暗号文字列を OpenSSL 暗号文字列形式で入力していることを確認してください。
- また、OpenSSH 形式の暗号またはアルゴリズムを **SSH Ciphers**フィールドに、 **SSH MAC** フィールドに、 **SSH 鍵交換** フィールドに入力します。
- 推奨される暗号 （81 ページ）を確認してください。

異なるセキュアインターフェイスで暗号文字列を設定するには、「暗号制限」セクションを参照してください。

手順

ステップ 1 Cisco Unified OS の管理から、 **セキュリティ** > **暗号管理**を選択します。
[暗号管理] ページが表示されます。

ステップ 2 **All TLS**、 **SIP TLS**、または **HTTPS TLS で暗号文字列を設定するには** フィールドの **暗号文字列** フィールドに OpenSSL 暗号文字列形式の暗号文字列を入力してください。

ステップ 3 次のフィールドで暗号文字列を設定しない場合:

- **すべての TLS または HTTPS TLS** フィールド: HTTPS TLS インターフェースポート (8443) は、 **エンタープライズパラメータ** (HTTPS 暗号) ページから設定を取得します。
- **すべての TLS または SIP TLS** フィールド—SIP インターフェースポート (5061) は、暗号化モードで **エンタープライズパラメータ** (TLS 暗号) ページから設定を取得し、認証モードでは NULL-SHA 暗号を使用します。

（注）
HTTPS TLS または **SIP TLS** フィールドで暗号文字列を設定しない場合、システムはデフォルトで **すべての TLS** フィールドから設定を取得します。

OpenSSL 暗号文字列形式の詳細は、 https://www.openssl.org/docs/man1.0.2/apps/ciphers.html を参照してください。

ステップ 4 **[SSH 暗号] フィールドで暗号文字列を設定するには、[暗号文字列フィールド]に OpenSSH 暗号文字列形式で暗号文字列を入力します。**

SSH 暗号用の OpenSSH 暗号文字列形式の詳細は、 https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html を参照してください。

[SSH 暗号] フィールドで暗号文字列を設定しない場合、デフォルトで次の暗号がすべての SSH 接続に適用されます:

FIPS モード：

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

非 FIPS モード：

```
aes128-ctr, aes192-ctr, aes256-ctr,
aes128-gcm@openssh.com, aes256-gcm@openssh.com
```

ステップ 5 キー交換アルゴリズムを [**SSH キー交換**] フィールドに設定するには、アルゴリズム文字列を OpenSSH 文字列形式で **アルゴリズム文字列** フィールドに入力します。

SSH 鍵交換のための OpenSSH アルゴリズム文字列形式の詳細は、 https://datatracker.ietf.org/doc/rfc9142/を参照してください。

[**SSH 鍵交換**] フィールドで鍵交換アルゴリズムを設定していない場合、デフォルトで次の鍵交換アルゴリズムがすべての SSH 接続に適用されます:

FIPS モード：

```
diffie-hellman-group1-sha1,diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

非 FIPS モード：

```
diffie-hellman-group1-sha1, diffie-hellman-group14-sha1,
diffie-hellman-group-exchange-sha1,diffie-hellman-group-exchange-sha256,
ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521
```

ステップ 6 MAC アルゴリズムを **SSH MAC** フィールドに設定するには、アルゴリズム文字列を OpenSSH 文字列形式で **アルゴリズム文字列** フィールドに入力します。

SSH MAC の OpenSSH アルゴリズム文字列形式に関する詳細は、 https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html を参照してください。

SSH MAC **フィールドで MAC アルゴリズムを設定しない場合、デフォルトで次の MAC アルゴリズムがすべての SSH 接続に適用されます。**

FIPS モード：

```
hmac-sha1
```

非 FIPS モード：

```
hmac-sha1
```

ステップ 7 **[保存（Save）]** をクリックします。

（注）
暗号拡張文字列 および **アルゴリズム拡張文字列** フィールドを編集することはできません。

システムは、 **All TLS**、 **SIP TLS**、 **HTTPS TLS** 、および **SSH Ciphers** フィールドに入力し、**暗号拡張文字列** フィールドに自動的に暗号が入力されますの暗号化を検証します。

[**暗号文字列**] フィールドに無効な暗号を入力すると、 **暗号拡張文字列** フィールドには自動入力されず、次のエラーメッセージが表示されます。

入力した暗号文字列は無効です。

システムは [**SSH キー交換**] および **SSH MAC** フィールドのアルゴリズムを検証し、 **アルゴリズム拡張文字列** フィールドに自動的にアルゴリズムを入力します。

[**アルゴリズム文字列**] フィールドに無効なアルゴリズムを入力すると、**[アルゴリズム拡張文字列]** フィールドは自動的に入力されず、次のエラーメッセージが表示されます。

無効なアルゴリズム文字列を入力しました。

（注）
暗号拡張文字列 および **アルゴリズム拡張文字列** フィールドに自動入力された暗号またはアルゴリズムは、有効な暗号またはアルゴリズムではありません。 システムは **暗号拡張文字列** または **アルゴリズム拡張文字列** フィールドから暗号またはアルゴリズムを選択します。

対応するフィールドで暗号を設定した場合、それぞれのサービスを再起動するか再起動する必要があります。

表 *13*：設定された暗号とそれに対応するアクション

設定された暗号フィールド	操作
すべて	クラスター内のすべてのノードを再起動して、暗号文字列を有効にします。
HTTPS TLS	暗号文字列を有効にするために、すべてのノードで Cisco Tomcat サービスを再起動します。
SIP TLS	暗号文字列を有効にするために、すべてのノードで Unified Communications Manager サービスを再起動してください。
SSH 暗号	クラスター内のすべてのノードを再起動して、暗号文字列を有効にします。
SSH キー交換 または **SSH MAC**	クラスター内のすべてのノードを再起動してアルゴリズム文字列を有効にします。

（注） **[暗号管理（Cipher Management）]** ページの **[暗号文字列（Cipher String）]** フィールドに暗号を入力することで有効にできます。 それらを入力しない場合、アプリケーションでサポートされているすべてのデフォルトの暗号が有効になります。 ただし、 **暗号管理** ページの **暗号文字列** フィールドに特定の弱い暗号を入力しないことにより、それらも無効にできます。

暗号の制限

暗号管理設定ページでは任意の数の暗号を設定できますが、各アプリケーションには、そのインターフェイスでサポートされている暗号のリストがあります。 例えば、**すべてのTLS**インターフェイスで ECDHE、DHE またはECDSA ベースの暗号が表示される場合がありますが、Unified Communications Manager などのアプリケーションでは、EC カーブまたはDHE アルゴリズムはこのアプリケーションのインターフェイスに対して有効ではないため、このような暗号をサポートしていない場合があります。 個々のアプリケーション インターフェイスでサポートされている暗号のリストの詳細については、「アプリケーションの暗号のサポート」のセクションを参照してください。

（注） [暗号管理（Cipher Management）]ページで設定された暗号を使用してクラスタをアップグレードする場合は、ALL フィールドと HTTPS フィールドの間に少なくとも 1 つの共通暗号を設定してください。

（注） いずれかのノードがクラスターから切断されていて、暗号を設定する場合、パブリッシャノードと切断されたノードの両方で暗号を更新していることを確認してください。

代わりに、クラスタが再確立されて同じ暗号設定を持つすべてのノードを同期した後で、パブリッシャノードで暗号を再度設定できます。

GUIでの検証

暗号管理ページの暗号は、OpenSSL のガイドラインに従って検証されます。 たとえば、ALL:BAD:!MD5と設定されている暗号の場合、「不良」は暗号一式として認識されていなくても、暗号構文は有効であると見なされます。 OpenSSLは、これを有効な文字列と見なします。AES128_SHA が AES128-SHA (ハイフンではなく下線) を使用して設定されている場合、OpenSSL はこれを無効な暗号スイートとして識別します。

認証モード (NULL 暗号)

アプリケーション インターフェイスが NULL の暗号を使用している場合は、**暗号管理**ページの **ALL TLS** または **SIP TLS** フィールドに暗号リストを設定することによって、NULL 暗号のサポートを無効にすることができます。

NULL 暗号を使用するアプリケーションインターフェイスの例は次のとおりです。

- **すべての TLS インターフェイス（All TLS Interface）**：**[TLS コンテキストの設定（TLS Context Configuration）]** ページ経由の IM and Presence の Unified Communications Manager SIP プロキシ。
- **SIP TLS インターフェイス:** SIP または SCCP で、いずれかの**デバイスセキュリティ プロファイル**が**認証済み**モードに設定されている場合に、SIP または SCCP が経由します。

NULL 暗号を使用する必要がある場合は、これら 2 つのインターフェイスのいずれについても暗号を設定しないでください。

オーバーライド機能

暗号管理 (Cipher Management) ページの設定により、各アプリケーションと、暗号が設定されているその他の場所のデフォルト設定が上書きされます。つまり、[**Cipher Management**]ページで暗号が設定されていない場合は、すべてのインターフェイスの元の機能が保持されます。

たとえば、**エンタープライズパラメータ**「**TLS の暗号**」が、サポートされ「ているすべて」の暗号**を使用**して設定され「ていて、*[*暗号管理*]* ページが暗号によって構成されている場合、*AES256-GCM-SHA384: AES256-SHA256*」**すべての TLS**インターフェイスで、すべてのアプリケーション SIP インターフェイスは「*AES256-gcm-SHA384: AES256-sha256*」暗号のみをサポートし、**エンタプライズパラメータ**値は無視されます。

アプリケーションの暗号のサポート

次の表は、アプリケーションインターフェイスと、TLS および SSH インターフェイスでサポートされているすべての対応する暗号、およびアルゴリズムを示しています。

表 *14 : TLS* 暗号のための *Unified Communications Manager* の暗号サポート

アプリケーション/プロセス	プロトコル	Port	サポート対象の暗号方式
Cisco CallManager	TCP/TLS	2443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256:AES128-SHA: ECDHE-RSA-AES256-SHA:
DRS	TCP/TLS	4040	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:

アプリケーション/プロセス	プロトコル	Port	サポート対象の暗号方式
Cisco Tomcat	TCP/TLS	8443 / 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco CallManager	TCP/TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco CTL Provider （注） Cisco CTL Provider は、リリース 14SU3 以降では使用できません。	TCP/TLS	2444	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:

アプリケーション/プロセス	プロトコル	Port	サポート対象の暗号方式
Cisco 認証局プロキシ機能	TCP/TLS	3804	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA
CTIManager	TCP/TLS	2749	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco 信頼検証サービス	TCP/TLS	2445	AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES256-SHA384: ECDHE-RSA-AES128-SHA256
Cisco クラスタ間検索サービス	TCP/TLS	7501	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
安全な設定ダウンロード (HAPROXY)	TCP/TLS	6971, 6972	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA:

アプリケーション/プロセス	プロトコル	Port	サポート対象の暗号方式
認証済み UDS 連絡先の検索	TCP/TLS	9443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA:

表 *15 : Unified Communications Manager IM* およびプレゼンス暗号サポートが *TLS* の暗号でサポートされています

アプリケーション/プロセス	プロトコル	Port	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	5061	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256: AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco SIP Proxy	TCP/TLS	5062	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384: AES256-SHA256:AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:

アプリケーション/プロセス	プロトコル	Port	サポート対象の暗号方式
Cisco SIP Proxy	TCP/TLS	8083	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco Tomcat	TCP/TLS	8443, 443	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: DHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES256-SHA256: DHE-RSA-AES256-SHA: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES128-SHA256: DHE-RSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-SHA384: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA:
Cisco XCP XMPP Federation Connection Manager	TCP/TLS	5269	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:

アプリケーション/プロセス	プロトコル	Port	サポート対象の暗号方式
Cisco XCP Client Connection Manager	TCP/TLS	5222	ECDHE-RSA-AES256-GCM-SHA384: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: ECDHE-ECDSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-RSA-AES128-SHA: ECDHE-ECDSA-AES128-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:

表 *16 : SSH* 暗号の暗号サポート

Service	暗号/アルゴリズム
SSH サーバ	• 暗号方式 aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC アルゴリズム： hmac-sha2-256 hmac-sha2-512 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512

Service	暗号/アルゴリズム
SSH クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC アルゴリズム： hmac-sha2-256 hmac-sha2-512 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512
DRS クライアント	• 暗号： aes256-ctr aes128-ctr aes192-ctr • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1 （注） Unified CM サーバーで暗号管理機能を設定している場合、Kex アルゴリズム diffie-hellman-group-exchange-sha256、diffie--group-exchange-sha1、および diffie-hellman-group1-sha1 はリリース 12.5(1)SU4 でサポートされません。暗号が設定されていない場合、DRS クライアントは次のアルゴリズムを使用します。

Service	暗号/アルゴリズム
SFTP クライアント	• 暗号： aes128-ctr aes192-ctr aes256-ctr • MAC アルゴリズム： hmac-sha2-256 hmac-sha1 • KEX アルゴリズム： ecdh-sha2-nistp521 ecdh-sha2-nistp384 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1
エンドユーザ	hmac-sha512 SHA-256 - Hashing (salted)
DRS バックアップ/ RTMT SFTP	AES-128 - Encryption
アプリケーションユーザ	AES-256 - Encryption

暗号の制限

暗号管理ページでは、OpenSSL または OpenSSH がサポートする暗号を設定できます。 ただし、暗号の一部は、偶発的なデータが偶発的に公開されることを回避するために、Cisco のセキュリティ標準に基づいて内部的に無効になっています。

[**Cipher Management**] ページで暗号を設定すると、次の暗号が基本的に無効になります。

TLS を無効にした暗号

```
EDH-RSA-DES-CBC-SHA:EDH-DSS-DES-CBC-SHA:ADH-DES-CBC-SHA:
DES-CBC-SHA:KRB5-DES-CBC-SHA:KRB5-DES-CBC-MD5:EXP-EDH-RSA-DES-CBC-SHA:
EXP-EDH-DSS-DES-CBC-SHA:EXP-ADH-DES-CBC-SHA:EXP-DES-CBC-SHA:EXP-RC2-CBC-MD5:
EXP-KRB5-RC2-CBC-SHA:EXP-KRB5-DES-CBC-SHA:EXP-KRB5-RC2-CBC-MD5:EXP-KRB5-DES-CBC-MD5:
EXP-ADH-RC4-MD5:EXP-RC4-MD5:EXP-KRB5-RC4-SHA:EXP-KRB5-RC4-MD5:ADH-AES256-GCM-SHA384:
ADH-AES256-SHA256:ADH-AES256-SHA:ADH-CAMELLIA256-SHA:ADH-AES128-GCM-SHA256:ADH-AES128-SHA256:
ADH-AES128-SHA:ADH-SEED-SHA:ADH-CAMELLIA128-SHA:ADH-DES-CBC3-SHA:ADH-RC4-MD5:
AECDH-AES256-SHA:AECDH-AES128-SHA:AECDH-DES-CBC3-SHA:AECDH-RC4-SHA:AECDH-NULL-SHA:
DES-CBC3-MD5:IDEA-CBC-MD5:RC2-CBC-MD5:RC4-MD5:ECDHE-RSA-RC4-SHA:ECDHE-ECDSA-RC4-SHA:
ECDH-RSA-RC4-SHA:ECDH-ECDSA-RC4-SHA:RC4-SHA:RC4-MD5:PSK-RC4-SHA:KRB5-RC4-SHA:
KRB5-RC4-MD5:IDEA-CBC-SHA:KRB5-IDEA-CBC-SHA:KRB5-IDEA-CBC-MD5:DHE-RSA-SEED-SHA:
DHE-DSS-SEED-SHA:SEED-SHA:KRB5-DES-CBC3-MD5:NULL-MD5:PSK-AES256-CBC-SHA:
PSK-AES128-CBC-SHA:PSK-3DES-EDE-CBC-SHA:ECDHE-RSA-NULL-SHA:ECDHE-ECDSA-NULL-SHA:
ECDH-RSA-NULL-SHA:ECDH-ECDSA-NULL-SHA:NULL-SHA256:NULL-SHA
```

SSH を無効にした暗号

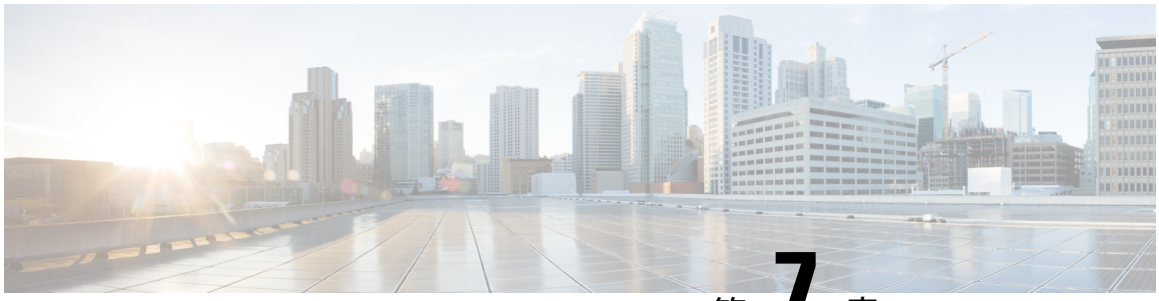
```
3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,rijndael-cbc@lysator.liu.se
```

SSH が無効になっている KEX アルゴリズム

```
curve25519-sha256@libssh.org,gss-gex-sha1-,gss-group1-sha1-,gss-group14-sha1-
```

SSH が無効になっている MAC アルゴリズム

```
hmac-sha1-etm@openssh.com,hmac-sha2-256-etm@openssh.com
```



第 7 章

安全なトーンとアイコン

- セキュアなトーンとアイコンの概要 （95 ページ）
- 安全なアイコンとトーンのヒント （98 ページ）
- セキュアなアイコンとトーンの設定タスク （100 ページ）
- セキュリティ通話とトーンの制限と制約 （102 ページ）

セキュアなトーンとアイコンの概要

安全なアイコンと安全なトーンは、通話のセキュリティ状況を警告する音声と視覚的なインジケータを提供します。 これらの機能は両方とも、通話のセキュリティ レベルについて通話参加者に警告するため、参加者は機密情報の交換が安全かどうかを知ることができます。

- セキュア アイコン: 通話のセキュリティ レベルを示すために電話機に表示されるアイコンです。
- セキュアなトーン: コールの開始時に再生される 2 秒間のトーン音で、コールがセキュアか非セキュアかを示します。

セキュアなアイコン

セキュリティアイコンは、電話のディスプレイに表示される視覚的なインジケータを提供し、コールがセキュアか非セキュアかを知らせます。 アイコンは、電話の通話時間タイマーの隣に表示されます。

セキュリティアイコンとその意味を次の表に示します:

表 *17:* セキュアなアイコン

セキュリティアイコン	セキュリティ レベル（**Security Level**）	説明
ロック 	暗号化されたコール	通話シグナリング (TLS 使用) と通話メディア (SRTP 使用) の両方が暗号化されます。 （注） 常に音声ストリームが暗号化されている必要があり、その場合のみ暗号化アイコンが電話に表示されます。 追加のメディア ストリーム (ビデオ、BFCP および iX チャネル) の暗号化は、コール セキュア ステータス ポリシー パラメータを構成する方法に応じて必要な場合があります。 既定値では、音声とビデオの両方のストリームが暗号化されている限り、メディアは暗号化されていると見なされます。
シールド 	認証された通話	コールシグナリングはTLSで暗号化されています。コールメディアは暗号化されていないか、部分的に暗号化されています。 たとえば、音声は暗号化されますが、ビデオは暗号化されません。 しかし、通話セキュアステータスポリシーには、通話のステータスが [暗号化（Encrypted）] になるには、両方が暗号化されている必要があることが示されています。
アイコンなし	非セキュア コール	認証されていないデバイスで非セキュアな音声とビデオ

追加情報

- 一部の電話モデルはロック アイコンのみを表示し (暗号化)、盾アイコンは表示されません (認証済み)。
- コールのセキュリティ ステータスは、ポイントツーポイント、クラスタ内、クラスタ間、およびマルチホップ コールに対して変更できます。 SCCP 回線、SIP 回線、H.323 信号トーンは、参加エンドポイントへのコール セキュリティ ステータス変更の通知をサポートしています。
- 電話会議およびバージコールの場合、セキュリティアイコンは電話会議のセキュリティステータスを表示します。

セキュア トーンの概要

セキュアトーンは、保護された電話で通話の開始時に再生されるように構成できます。 トーンは、通話中の他のデバイスがセキュアかどうかを警告します。他のデバイスがセキュアではな

い場合はノンセキュアのトーンが聞こえ、他のデバイスがセキュアな場合はセキュアなトーンが聞こえます。

すべての電話に表示されるセキュア アイコンとは異なり、セキュア トーンは保護されたデバイスとして設定されている電話でのみ再生されます。 通話中の両方の電話がセキュアで、ただ一方の電話だけが保護デバイスである場合、保護デバイスの電話だけがトーンを聞きます。

次の表では、トーンのタイプとそれぞれの意味を示します。

表 *18*：セキュア トーン

セキュア トーン	説明
長いビープ音 3 回	セキュアコール 他の電話はセキュアフォンです。
6 回の短いビープ音	非セキュアな通話です。 他の電話は非セキュアです。

通話中の変更

通話中に通話のセキュリティステータスが変更された場合、新しいセキュリティステータスを知らせるために、通話中に新しくセキュアまたは非セキュアトーンが再生されます。 保護されたデバイスを使用しているユーザにのみ、トーン音が聞こえます。

通話の種類

セキュアトーンは、次のタイプの通話に対して動作します。

- クラスタ間のコール（IP 間）
- 保護されているとみなされるクラスタ間コール
- MGCP ゲートウェイ E1 接続を介した IP から TDM へのコール (MGCP ゲートウェイは保護デバイスである必要があります)

セキュアな電話コールの識別

自分の電話と相手側の電話がセキュア コール用に設定されている場合、セキュア コールを確立して識別することができます。 セキュアな会議ブリッジのセットアップ後、電話会議ではセキュアなコールがサポートされます。

セキュアな電話から発信するとセキュアな通話が確立されます (セキュアモード)。 セキュア アイコンは電話スクリーンに表示され、その電話機がセキュア コール用に設定されていることを示します。しかし、接続されている他の電話機もセキュアであることを意味しません。

そのコールが別のセキュアな電話機に接続された場合は、ユーザにセキュリティ トーンが聞こえ、通話の両端が暗号化および保護されていることを示します。

（注） コールがセキュアでない電話に接続されると、セキュリティ トーンは聞こえません。

安全なアイコンとトーンのヒント

セキュアなコールは、2台の電話機の間でサポートされます。保護された電話では、セキュアコールが設定されている場合、電話会議、共有回線、エクステンションモビリティなどの機能を利用できません。保護された電話の発信者だけがセキュアおよび非セキュア インディケーション トーンを聞くことができます。保護されていない電話の発信者には、これらのトーンが聞こえません。ビデオ コールの場合、システムは保護されたデバイスでセキュアおよび非セキュア通知トーンを再生します。

セキュリティ アイコンをサポートするすべての電話に、コール セキュリティ レベルが表示されます。

- 認証のシグナリング セキュリティ レベルを持つコールに対しては、盾アイコン が表示されます。盾のアイコンは、Cisco IP端末間のセキュアな接続を示します。このアイコンは、デバイスが暗号化シグナリングを使用していることを示します。
- 電話は、暗号化されたメディアでの 通話に対してロックアイコンを表示します。このアイコンは、デバイスが暗号化シグナリングと暗号化メディアを使用していることを示します。
- 一部の電話モデルにはロック アイコンのみが表示されます。

コールのセキュリティ ステータスは、ポイントツーポイント、クラスタ内、クラスタ間、およびマルチホップ コールに対して変更できます。SCCP回線、SIP回線、H.323シグナリングは、参加エンドポイントへのコール セキュリティ ステータス変更の通知をサポートしています。

保護された電話はセキュアまたはノンセキュアの通知トーンのみを再生します。保護されていない電話機は、インディケーショントーンを決して再生しません。コール中に全体的なコールステータスが変化すると、インジケーション トーンも変化し、保護された電話で適切なトーンが再生されます。

保護された電話が適切なトーンを再生するいくつかのシナリオを以下に示します。

- **[セキュア インディケーション トーンの再生（Play Secure Indication Tone）]** オプションを有効にした場合。
- エンドツーエンドのセキュアなメディアが確立され、コールステータスがセキュアになった場合、電話機はセキュアインディケーション トーン（間に小休止を伴う3回の長いビープ音）を再生します。
- エンドツーエンド非セキュア メディアが確立され、コール ステータスが非セキュアの場合、電話は非セキュアを示すトーンを再生します。短いビープ音が6回と一時停止になります。
- **[セキュア インディケーション トーンの再生（Play Secure Indication Tone）]** オプションを無効にすると、トーンは再生されません。

サポート対象デバイスのセキュアトーン

この手順を使用してセキュアトーンをサポートする電話のリストを取得します。

手順

ステップ 1 Cisco Unified Reporting から **[システムレポート（System Reports）]** をクリックします。
ステップ 2 **[Unified CM 電話機能リスト（Unified CM Phone Features List）]** をクリックします。
ステップ 3 [**新規レポートの生成**] をクリックします。
ステップ 4 **機能** ドロップダウンリストから **セキュアトーン**を選択します。
ステップ 5 [送信（Submit）]をクリックします。

Cisco Unified Reporting の使用方法の詳細は、 Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。

保護されたデバイスのセキュアトーン

Cisco Unified IP 電話で保護デバイスとして設定できるのは、サポートされている Unified Communications ManagerおよびMGCP E1 PRIゲートウェイだけです。 Unified Communications Manager は、システムがコールの保護状態を判断したときに、セキュアおよび非セキュアの通知音を再生するようにMGCP IOSゲートウェイを指示することもできます。

セキュアおよび非セキュアインジケータトーンを使用して、次のタイプのコールを発信できます。

- クラスター内 IP から IP への通話
- システムが保護していると判断したクラスタ間呼び出し
- 保護された MGCP E1 PRI ゲートウェイ経由の IP と時分割多重化（TDM）コール

ビデオコールの場合、システムにより保護対象デバイスでセキュア通知トーンと非セキュア通知トーンが再生されます。

保護対象デバイスは以下の機能を提供します。

- SCCP または SIP を実行する電話機を保護対象デバイスとして設定できます。
- 保護されたデバイスは、暗号化または非暗号化のいずれかの保護されていないデバイスに発信できます。 このような場合、コールは保護されていないものとして指定され、システムはコールに関係している電話機で非セキュア通知トーンを再生します。
- 保護された電話が別の保護された電話を呼び出し、メディアが暗号化されていない場合、システムはノンセキュア インジケータ トーンをコール中の電話に再生します。

電話機を保護された状態に設定するには、**Cisco Unified CM Administration** ページの **[保護されたデバイス（Protected Device）]** チェックボックスを **[電話機の設定（Phone Configuration）]** ウィンドウでオンにしてください。

セキュアなアイコンとトーンの設定タスク

次のタスクを使用して、セキュアなアイコンとセキュアなトーンを設定することができます:

手順

	コマンドまたはアクション	目的
ステップ 1	通話のセキュリティステータスポリシーのセットアップ	通話セキュア ステータス ポリシーは、セキュア アイコン機能が通話を暗号化として表示するために、通話内のどのメディア ストリームを暗号化する必要があるかを示します。 既定では、音声とビデオ (ビデオ コールの場合) は両方とも暗号化する必要があります。 設定を再構成して BFCP と iX チャネルも考慮することができます。
ステップ 2	セキュリティ指示音を有効にする	保護された電話でセキュア表示トーンを有効にします。
ステップ 3	電話を保護されたデバイスとして設定する	でサポートされている Cisco Unified IP 電話を保護されたデバイスとして設定してください Unified Communications Manager。

セキュアアイコンポリシーのセットアップ

通話セキュア ステータス ポリシーは、電話のセキュア ステータス アイコンの表示を制御します。 ポリシーオプションは以下のとおりです。

- BFCP および iX アプリケーション ストリームを除くすべてのメディアを暗号化する必要があります

  これがデフォルト値です。 通話のセキュリティ ステータスは、BFCP および iX アプリケーション ストリームの暗号化ステータスに依存しません。

- iX アプリケーション ストリームを除くすべてのメディアを暗号化する必要があります

  通話のセキュリティ ステータスは、iX アプリケーション ストリームの暗号化ステータスには依存しません。

- BFCP アプリケーション ストリームを除くすべてのメディアを暗号化する必要があります

通話のセキュリティ状況は、BFCP の暗号化状況に依存しません。

- セッション中のすべてのメディアを暗号化する必要があります

  通話のセキュリティ ステータスは、確立された電話セッションのすべてのメディア ストリームの暗号化ステータスに依存しています。

- 音声のみを暗号化する必要があります

  通話のセキュリティ状況は、音声ストリームの暗号化によって異なります。

（注） このポリシーの変更は、電話でのセキュア アイコンの表示とセキュア トーンの再生に影響を与えます。

手順

ステップ 1 Cisco Unified Communications Manager Administration で、**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

ステップ 2 サーバとサービスの **選択** ペインから、サーバと CallManager サービスを選択します。

ステップ 3 **[クラスタ全体のパラメータ（機能 - 通話セキュアステータスポリシー）（Clusterwide Parameters (Feature - Call Secure Status Policy)）]** ペインに移動します。

ステップ 4 **[セキュア着信アイコン表示ポリシー（Secure Call Icon Display Policy）]** フィールドで、ドロップダウンメニューからポリシーを選択します。
ビデオ コールとセキュア トーンに影響を与えることを知らせる警告メッセージが表示されます。

ステップ 5 **[保存（Save）]** をクリックします。
ウィンドウが更新され、Unified Communications Manager は **[サービスパラメータ設定（Service Parameter Configuration）]** ページのポリシーを更新します。

クラスターの安全通知トーンを有効にする

セキュア・インジケーション・トーンは、コールの全体的なステータスが「保護」を示し、コールが暗号化されているとシステムが判断した場合に、セキュアな電話で再生されます。インディケーショントーンを True に設定する必要があります。

手順

ステップ 1 Cisco Unified Communications Manager Administration ページで、**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。

ステップ 2 [サーバとサービスの **選択**] ペインから、サーバと CallManager サービスを選択します。

ステップ 3 [**クラスター全体のパラメータ (機能 - Secure Tone)**] ペインに移動します。

ステップ 4 [**セキュア/非セキュア通話の状況を示すためのトーン音の再生**] を [**True**] に設定します。 既定では、 **False** になっています。

クラスタでセキュア指示音を設定した後、個々の電話を保護された電話として設定します。 保護された電話だけがセキュア トーンと非セキュア トーンを聞くことができます。

電話機の保護デバイスとしての設定

サポート対象の Cisco Unified IP Phones を保護対象デバイスとして Unified Communications Manager で設定できます。 保護された電話機の発信者だけがセキュアおよびセキュアでないインジケータトーンを聞くことができます。

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス] > [電話機]** を選択します。
電話のリストが表示されます。

ステップ 2 セキュア トーン パラメータを設定する電話をクリックします。

ステップ 3 [**端末情報**] ペインに移動して次の作業を行います:

1. **ソフトキーテンプレート** ドロップダウンリストから、 **標準保護電話を選択します。**

   （注）
   保護された電話機用の補足サービス ソフトキーのないソフトキー テンプレートを使用する必要があります。

2. [保護デバイス（Protected Device）] チェック ボックスをオンにします。

ステップ 4 [**プロトコル固有情報**] ペインに移動します。

ステップ 5 [**端末セキュリティプロファイル**] ドロップダウンリストから、[**電話セキュリティプロファイルの構成**] で構成済みの暗号化セキュリティ電話プロファイルを選択します。

ステップ 6 **[保存]** をクリックします。

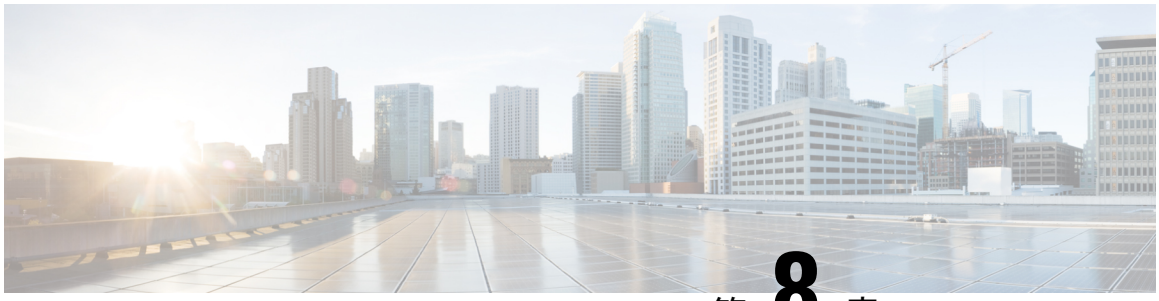
セキュリティ通話とトーンの制限と制約

以下は、セキュアコールとトーンに関する制限事項です。

表 *19 :* セキュアアイコンとセキュア音声信号 対話と制限

機能	連携動作と制限事項
H.323 トランク	セキュア アイコンは H.323 トランクではサポートされない

機能	連携動作と制限事項
通話の転送と保留	暗号化ロック アイコンは、通話の転送または保留などのタスクを実行するときに、電話に表示されない場合があります。 これらのタスクに関連付けられたメディア ストリームが暗号化されていない場合、ステータスが暗号化済みから非セキュアに変更されます。
PSTN 通話	PSTN を含む通話の場合、セキュリティ アイコンは通話の IP ドメイン部分のみのセキュリティ ステータスを表示します。
割込み	セキュアなアイコン: • セキュアではない、または認証された Cisco IP 電話は、暗号化されたコールに割り込む可能性があります。 セキュリティアイコンは電話会議のセキュリティ状況を示します。 セキュア トーンあり: • 発信者がセキュアな SIP コールにバージすると、システムは保留時トーンを提供し、 Unified Communications Manager はトーンの間、コールを非セキュアとして分類します。 • 発信者がセキュアな SCCP コールにバージする場合、システムはターゲット デバイスで内部のトーン再生メカニズムを使用し、ステータスはセキュアなままです。



第 8 章

Certificate Authority Proxy 機能

- 認証局プロキシ機能（CAPF）の概要 （105 ページ）
- 認証局のプロキシ機能の構成タスクフロー （107 ページ）
- 認証局のプロキシ機能の管理タスクフロー （116 ページ）
- CAPF システムの相互作用 （119 ページ）

認証局プロキシ機能（CAPF）の概要

認証局プロキシ 機能 (CAPF) は、Locally Significant Certificates (LSC) を発行し、エンドポイントを認証します。

CAPF サービスは Unified Communications Manager で実行され、以下のタスクを実行します:

- サポートされている Cisco Unified IP 電話 に LSC を発行します。
- 混合モード中に電話を認証します。
- 電話機用の既存の LSCs をアップグレードします。
- 表示およびトラブルシューティングを行うために電話の証明書を取得する。

CAPF サービス証明書

CAPF サービスは Unified Communications Manager のインストール時に自動的にインストールされ、CAPF 指定のシステム証明書が生成されます。

重要 次のメモはリリース 14SU2 以降にのみ適用されます。

（注） CAPF 証明書には、次のデフォルトの X509 拡張子が含まれている必要があります。

X509v3 の基本的制約:

CA:TRUE, pathlen:0

X509v3 キーの使用法:

デジタル署名、証明書署名

これらの拡張機能が CAPF 証明書に存在しない場合、TLS 接続エラーが発生します。

次のモードで動作するように CAPF を設定することができます。

表 *20 : CAPF* 実行モード

モード	説明
Cisco Authority Proxy 機能	デフォルトでは、CAPF サービスで Unified Communications Manager CAPF サービス署名 LSC を発行します。
オンライン CA	[オンライン CA (Online CA)]: 外部オンライン CA が「電話用 LSC」として署名している場合は、このオプションを使用します。CAPF サービスは、自動的に外部 CA に接続されます。証明書署名リクエスト（CSR）が手動で送信された場合、CA は署名し、CA の署名済み LSC を自動的に返します。 （注） オンライン CA は、ECDSA キー サイズでの CAPF 操作をサポートしません。
オフライン CA	オフライン CA: このオプションは、オフラインの外部 CA を使用して LSC for phone に署名する場合に使用します。 LSC を手動でダウンロードし、CA に提出し、準備ができたら CA 署名付き証明書をアップロードします。 （注） サードパーティの CA を使用して LSC に署名する場合は、 **オフライン CA** オプションの代わりに **オンライン CA** オプションをおすすめします。 **オンライン CA** は自動化され、より迅速になり、問題が発生する可能性が低くなります。

LSC を生成する前に、以下を確認してください。

- Unified Communications Manager リリース 12.5 以降。
- 証明書に CAPF を使用するエンドポイントを含む Cisco Unified IP 電話 および Jabber。
- CA が設定された Microsoft Windows Server 2012 および 2016。

- ドメイン ネーム サービス (DNS)

前提条件として、電話を認証する方法も決めてください。

LSC を必要なトラストストアに生成する前に、CA ルートおよび HTTPS 証明書をアップロードします。 インターネットインフォメーションサービス (IIS) は、HTTPS 証明書をホストします。 セキュア SIP connection では、HTTPS 証明書は CAPF-トラストを通過し、CA ルート証明書は CAPF トラストで Unified Communications Manager-トラストをたどります。 CA ルート証明書は、証明書署名要求 (CSRs) への署名に使用されます。

以下は、さまざまな証明書をアップロードするシナリオです。

表 *21* : 証明書のアップロードシナリオ

シナリオ	アクション
CA ルートおよび HTTPS証明書は同じです。	CA ルート証明書をアップロードする。
CA ルートと HTTPS の証明書は異なり、HTTPS 証明書は同じ CA ルート証明書によって発行されます。	CA ルート証明書をアップロードする。
CA ルート証明書は異なる中間 CA および HTTPS証明書を発行します。	CA ルート証明書をアップロードする。
CA ルートと HTTPS の証明書は異なり、同じ CA ルート証明書によって発行されます。	CA ルートおよび HTTPS 証明書をアップロードする。

（注） スケジュールされたメンテナンス期間中にCAPFを使用することを推奨します。複数の証明書を同時に生成すると、コール処理が中断される可能性があるためです。

認証局のプロキシ機能の構成タスクフロー

次のタスクを実行して、証明機関プロキシ機能 (CAPF) サービスがエンドポイント用 LSCs を発行するように設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	サードパーティの認証局のルート証明書のアップロード	LSC にサードパーティの CA 署名を適用する場合は、CA ルート証明書チェーンを CAPF 信頼ストアにアップロードします。 それ以外の場合は、この作業をスキップできます。
ステップ 2	認証局（CA）ルート証明書のアップロード （109 ページ）	CA ルート証明書をUnified Communications Manager信頼ストアにアップロードします。
ステップ 3	オンライン認証局の設定 （110 ページ）	電話機 LSC 証明書を生成するには、次の手順を使用します。
ステップ 4	オフライン認証局の設定の設定	オフライン CA を使用して電話機 LSC 証明書を生成するには、次の手順を使用します。
ステップ 5	CAPF サービスをアクティブ化または再起動する	CAPF システム設定を構成した後に、重要な CAPF サービスをアクティブにします。
ステップ 6	次のいずれかの手順を使用して、Unified Communications Managerの CAPF 設定を構成します。 • CAPD 設定をユニバーサル デバイス テンプレートで設定します。 （112 ページ） • バルク Admin による CAPF 設定の更新 （114 ページ） • 電話機の CAPF 設定の設定 （115 ページ）	次のオプションのいずれかを使用して、CAPF 設定を電話機の設定に追加します。 • まだ LDAP ディレクトリを同期していない場合、CAPF 設定をユニバーサルデバイステンプレートに追加し、初期 LDAP 同期を使用して設定を適用することができます。 • 一括管理ツールを使用すると、1 回の操作で多数の電話機に CAPF 設定を適用できます。 • CAPF 設定を電話機ごとに適用することができます。
ステップ 7	キープアライブ タイマーの設定 （116 ページ）	ファイアウォールによってタイムアウトにならないように、CAPF エンドポイント接続のキープアライブ値を設定します。 デフォルト値は 15 分です。

サードパーティの認証局のルート証明書のアップロード

CA ルート証明書を CAPF 信頼ストアと Unified Communications Manager信頼ストアにアップロードして、外部 CA を使用して LSC 証明書に署名します。

（注） サードパーティ CA を使用して LSCs に署名しない場合は、このタスクをスキップできます。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書目的]** ドロップダウンリストで、**[CallManager 信頼]** を選択します。

ステップ 4 証明書の説明を [説明（Description）] に入力します。 たとえば、**外部 LSC 署名 CA の証明書などです。**

ステップ 5 [参照（Browse）]をクリックしてファイルに移動してから、[開く（Open）]をクリックします。

ステップ 6 [アップロード（Upload）]をクリックします。

ステップ 7 このタスクを繰り返して、証明**書の目的で**使用**される発信者管理者の信頼に証明書をアップロードします。**

認証局（CA）ルート証明書のアップロード

（注） 中間またはルート CA 証明書の共通名に「CAPF-」部分文字列が含まれていないことを確認してください。「CAPF-」共通名は、CAPF 証明書用に予約されています。

手順

ステップ 1 Cisco Unified OS の管理から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[証明書/証明書チェーンのアップロード]** をクリックします。

ステップ 3 **[証明書目的（Certificate Purpose）]** ドロップダウンリストで、**[CallManager 信頼（CallManager-trust）]** を選択します。

ステップ 4 証明書の説明を [説明（Description）] に入力します。 たとえば、**外部 LSC 署名 CA の証明書などです。**

ステップ 5 [参照（Browse）]をクリックしてファイルに移動してから、[開く（Open）]をクリックします。

オンライン認証局の設定

オンライン CAPF を使用して電話機 LSC を生成するには、Unified Communications Managerにあるこの手順を使用します。

（注） FIPS 対応モードでは、オンライン CAPF および CAPFv3 がサポートされません。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[サービス パラメータ（Service Parameters）]** の順に選択します。

ステップ 2 **[サーバ]** ドロップダウン リストから、[Cisco 認証局プロキシ 機能（アクティブ）] サービスを選択します。

ステップ 3 [サービス（Service）]ドロップダウン リストから、[Cisco 認証局プロキシ機能（アクティブ）（Cisco 認証局プロキシ 機能 (Active)）]を選択します。 サービス名の横に「Active」と表示されることを確認します。

ステップ 4 [エンドポイントへの証明書発行者（Certificate Issuer to Endpoint）]ドロップダウン リストから、[オンラインCA（Online CA）]を選択します。 CA 署名付き証明書では、オンライン CA を使用することを推奨しています。

ステップ 5 **[証明書の有効期間（日数）]** フィールドに、CAPF が発行した証明書が有効である日数を表す数値を、1 ～ 1825 の間で指定します。

ステップ 6 **オンライン CA パラメータ** セクションで、次のパラメータを設定して、オンライン CA セクションへの接続を作成します。

- オンライン CA ホスト名 - サブジェクト名または共通名 (CN) は、HTTPS 証明書の完全修飾ドメイン名 (FQDN) と同じである必要があります。

  （注）
  設定されたホスト名は、Microsoft CA 上で実行されているインターネット インフォメーション サービス (IIS) によってホストされている HTTP の証明書の共通名 (CN) と同じです。

- オンライン CA ポート - オンライン CA のポート番号を入力します。例：443。
- オンライン CA テンプレート：テンプレートの名前を入力します。 Microsoft CA がテンプレートを作成します。
- オンライン CA タイプ：デフォルトのタイプである Microsoft CA を選択します。
- オンライン CA ユーザ名：CA サーバのユーザ名を入力します。

- オンライン CA パスワード：CA サーバのユーザ名のパスワードを入力します。

ステップ 7 残りの CAPF サービス パラメータを完了します。 サービスパラメータのヘルプ システムを表示するには、パラメータ名をクリックします。

ステップ 8 **[保存]** をクリックします。

ステップ 9 変更内容を有効にするには、**Cisco 認証局プロキシ 機能** サービスを再起動します。 Cisco Certificate Enrollment service を自動的に再起動します。

現在のオンライン CA の制限

- CA サーバが英語以外の言語を使用している場合、オンライン CA 機能は動作しません。CA サーバは英語でのみ応答します。
- オンライン CA 機能は、CA での mTLS 認証をサポートしていません。
- LSC 操作にオンライン CA を使用している場合、LSC 証明書に「デジタル署名」と「キー暗号化」のキー使用法が指定されていないと、デバイスのセキュア登録は失敗します。

オフライン認証局の設定の設定

オフライン CA を使用して電話機 LSC 証明書を生成することを決定した場合は、次の高度なプロセスに従うことができます。

（注） オフライン CA オプションを使用すると、オンライン Ca よりも時間がかかり、手動による手順が多くなります。 証明書の生成および送信プロセス中に問題 (たとえば、ネットワークの停止や電話機のリセットなど) が発生した場合は、プロセスを再起動する必要があります。

手順

ステップ 1 サードパーティ認証局からルート証明書チェーンをダウンロードします。

ステップ 2 Unified Communications Managerのルート証明書チェーンを必要な信頼(CallManager 信頼 CAPF 信頼)にアップロードします。

ステップ 3 オフライン CA に対して **Certificate Issue to Endpoint** サービスパラメータを設定すると、オフラインの CA を使用するように Unified Communications Manager を設定できます。

ステップ 4 お使いの電話機の LSC 用に **CSR** を生成します。

ステップ 5 認証局に**CSR** を送信します。

ステップ 6 **CSR** から署名付き証明書を取得します。

オフライン CA を使用して電話機 LSC を生成する方法の詳細な例については、「CUCM サードパーティ CA 署名付き LSCs 生成とインポート設定」を参照してください。

CAPF サービスをアクティブ化または再起動する

CAPF システムを設定した後に、重要な CAPF サービスをアクティブにします。 CAPF サービスがすでにアクティブ化されている場合は、再起動します。

手順

ステップ 1 Cisco Unified Serviceability から**[ツール]** > **[サービス アクティベーション]** を選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストからパブリッシャ ノードを選択し、[移動（Go）]をクリックします。

ステップ 3 **[セキュリティサービス]** ペインから、次の該当するサービスを確認します。

- **Cisco Certificate Enrollment Service**: オンラインCAを使用している場合はこのサービスのチェックをオンにし、そうでない場合はチェックを外したままにします。
- **Cisco Certificate Authority プロキシ機能**: このサービスをオフ (非アクティブ) にした場合は、チェックを入れます。 サービスがすでにアクティブ化されている場合は、再起動します。

ステップ 4 いずれかの設定を変更した場合、**[保存]** をクリックします。

ステップ 5 **Cisco 認証局プロキシ機能** サービスがすでにチェックされている場合は（アクティブ）、再起動します。

a) **[関連リンク]**ドロップダウン リストから**[コントロールセンター-ネットワークサービス]**を選択し、**[移動]** をクリックします。

b) **[セキュリティの設定（Security Settings）]** ペインから、**[Cisco 認証局プロキシ機能（Cisco Certificate Authority Proxy Function）]** サービスを確認し、**[再起動（Restart）]** をクリックします。

ステップ 6 次の手順のいずれかを実行して、個々の電話機に対して CAPF 設定を構成します。

a) CAPD 設定をユニバーサル デバイス テンプレートで設定します。 （112 ページ）

b) バルク Admin による CAPF 設定の更新 （114 ページ）

c) 電話機の CAPF 設定の設定 （115 ページ）

CAPD 設定をユニバーサル デバイス テンプレートで設定します。

CAPF設定をユニバーサルデバイステンプレートに設定するには、次の手順を実行します。テンプレートは、機能グループテンプレートの設定を使用して、LDAPディレクトリ同期に適用します。テンプレートのCAPF設定が、このテンプレートを使用する同期済みのすべてのデバイスに適用されます。

（注） Universal デバイステンプレートは、まだ同期されていない LDAP ディレクトリにしか追加することができません。 初期 LDAP 同期が発生した場合は、一括管理を使用して電話機を更新します。 詳細については、バルク Admin による CAPF 設定の更新 （114 ページ）を参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）] > [ユーザ/電話の追加（User/Phone Add）] > [ユニバーサルデバイステンプレート（Universal Device Template）]** を選択します。

ステップ 2 次のいずれかを実行します。

- **[検索]** をクリックし、既存のテンプレートを**選択**します。
- [新規追加] をクリックします。

ステップ 3 **認証局プロキシ機能（CAPF）の設定**領域の拡張

ステップ 4 [証明書の操作（Certificate Operation）] ドロップダウン リストで、[インストール/アップグレード（Install/Upgrade）] を選択します。

ステップ 5 **[認証モード]** ドロップダウンメニューで、デバイスを認証するオプションを選択します。

ステップ 6 認証文字列の使用を選択した場合は、**テキストボックス**に認証文字列を入力するか、**[**文字列の生成 ([文字列の生成])] をクリックして、システムによって文字列が生成されるようにします。

（注）
この文字列がデバイス上で設定されていない場合、認証は失敗します。

ステップ 7 残りのフィールドで、キー情報を設定します。 フィールドの詳細については、オンライン ヘルプを参照してください。

ステップ 8 **[保存]** をクリックします。

（注）
このテンプレートを使用するデバイスは、この手順で割り当てたのと同じ認証方法で構成されていることを確認してください。 それ以外の場合、デバイス認証は失敗します。 電話機の認証を設定する方法の詳細については、電話機のマニュアルを参照してください。

ステップ 9 このプロファイルを使用するデバイスにテンプレート設定を適用します。

a) ユニバーサルデバイステンプレートを Feature Group テンプレートの設定に追加します。
b) 機能グループテンプレートを、同期されていない LDAP ディレクトリ設定に追加します。
c) LDAP 同期を完了します。 CAPF 設定は、同期されているすべてのデバイスに適用されます。

機能グループテンプレートとLDAP ディレクトリ同期の設定の詳細については、Cisco Unified Communications Manager システム設定ガイドの「Configure End Users」セクションを参照してください。

バルク Admin による CAPF 設定の更新

一括管理の**電話機の更新**クエリを使用して、多数の既存の電話機の CAPF 設定と lsc 証明書を 1 回の操作で構成します。

（注） まだ電話機をプロビジョニングしていない場合は、一括管理の**[電話機の挿入]**メニューを使用して、CSV ファイルからの CAPF 設定で新しい電話機をプロビジョニングできます。 CSV ファイルから電話機を挿入する方法の詳細については、Cisco Unified Communications Manager 一括管理ガイドの「電話機の挿入」セクションを参照してください。

電話機は、この手順で追加する認証方法と文字列と同じように設定されていることを確認します。 それ以外の場合、お使いの電話機は CAPF に対して認証しません。 電話機で認証を設定する方法の詳細については、「電話機のマニュアル」を参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、以下を選択します。**バルク管理** > **電話機** > **電話機の更新** > **クエリ**

ステップ 2 フィルタオプションを使用して、更新する電話機に検索を制限し、**[検索]**をクリックします。

たとえば、**[電話機の検索場所]**ドロップダウンを使用して、LSC が特定の日付の前期限切れになるすべての電話機またはデバイスプール内の電話機を選択することができます。

ステップ 3 [次へ（Next）]をクリックします。

ステップ 4 **ログアウト/リセット/再起動**セクションから**[設定の適用]**を選択します。 ジョブを実行すると、CAPF アップデートは更新されたすべての電話に適用されます。

ステップ 5 [**証明機関プロキシ関数（capf）]**の情報で、**[**証明書の操作（Certificate Operation）] チェックボックスをオンにします。

ステップ 6 **[証明書の操作]** ドロップダウン リストから、**[インストール /アップグレード]** を選択して、新しい LSC 証明書を電話機にインストールします。

ステップ 7 **[認証モード]** ドロップダウンから、LSC インストール時に電話機を認証する方法を選択します。

（注）
電話機で同じ認証方法を設定します。

ステップ 8 **認証モード**として**認証文字列**で選択した場合は、次の手順のいずれかを実行します。

- 各デバイスに対して一意の認証文字列を使用する場合は、**各デバイスに対して一意の認証文字列を生成する**ことを確認してください。
- すべてのデバイスに同じ認証文字列を使用する場合は、**[認証文字列]**テキストボックスに文字列を入力するか、**[文字列の生成]** をクリックします。

ステップ 9 **[電話の更新（Update Phones）]** ウィンドウで **[CAPF の情報（Certification Authority Proxy Function（CAPF）Information）]** セクションの残りのフィールドを入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 10 **[ジョブ情報（Job Information）]** セクションで、**[今すぐ実行（Run Immediately）]**を選択します。

（注）
スケジュールされた時刻にジョブを実行する場合は、**[後で実行する]** を選択します。 ジョブのスケジュール設定の詳細については、Cisco Unified Communications Manager 一括管理ガイドの「スケジュールされたジョブの管理」セクションを参照してください 。

ステップ 11 [送信（Submit）]をクリックします。

（注）
この手順で **[設定の適用]** オプションを選択しなかった場合は、更新されたすべての電話機の **[電話機の設定]** ウィンドウで設定を適用します。

電話機の CAPF 設定の設定

個々の電話機の LSC 証明書の CAPF 設定を設定するには、次の手順を実行します。

（注） CAPF 設定を多数の電話機に適用するには、バルク管理または LDAP ディレクトリ同期を使用します。

電話機は、この手順で追加する認証方法と文字列と同じように設定します。 それ以外の場合、電話機は CAPF に対して自身を認証しません。 電話機で認証を設定する方法の詳細については、「電話機のマニュアル」を参照してください。

手順

ステップ 1 Cisco Unified CM Administration から、以下を選択します。**[デバイス]** > **[電話]**

ステップ 2 既存の電話機を選択するには、[検索（Find）]をクリックします。 **[電話設定]** ページが表示されます。

ステップ 3 **[認証局プロキシ機能 (CAPF) の情報]** ペインに移動します。

ステップ 4 **[証明書の操作]** ドロップダウン リストから、**[インストール /アップグレード]** を選択して、新しい LSC 証明書を電話機にインストールします。

ステップ 5 **[認証モード]** ドロップダウンから、LSC インストール時に電話機を認証する方法を選択します。

（注）
電話機は、同じ認証方法を使用するように設定されている必要があります。

ステップ 6 **[認証文字列]** で選択した場合は、テキスト文字列を入力するか、**[文字列の生成]** をクリックして、システムが文字列を生成するようにします。

ステップ 7 **[電話機の設定（Phone Configuration）]** ページで **[認証局プロキシ機能 (CAPF) の情報]** ペインの残りのフィールドに詳細を入力します。フィールドとその設定の詳細については、オンライン ヘルプを参照してください。

ステップ 8 **[保存（Save）]** をクリックします。

キープアライブ タイマーの設定

ファイアウォールによって接続がタイムアウトしないように、次の手順を実行して、CAPF-エンドポイント接続のクラスターワイドキープアライブタイマーを設定します。デフォルト値は 15 分です。各間隔の後、CAPF サービスは電話機にキープアライブ信号を送信して、接続を開いた状態にします。

手順

ステップ 1 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。

ステップ 2 `utils capt set keep_alive` CLI コマンドを実行します。

ステップ 3 5 ~ 60 (分) の間の数値を**入力**し、確定キーをクリックします。

認証局のプロキシ機能の管理タスクフロー

CAPF が設定され LSC 証明書が発行されたら、継続的に LSC 証明書を管理します。

手順

	コマンドまたはアクション	目的
ステップ 1	CAPF による LSC の生成	CAPF を設定し、設定した認証文字列を電話に追加します。キーと証明書の交換は、電話と CAPF の間で行われます。

	コマンドまたはアクション	目的
ステップ 2	古い LSC レポートの実行	Cisco Unified Reporting から無効な LSC レポートを実行します。 古い LSCs は、エンドポイント CSR への応答として生成された証明書ですが、古くなった LSCS がインストールされる前に新しい CSR が生成されたため、インストールされませんでした。
ステップ 3	保留中の CSR リストの表示	保留中の CAPF CSR ファイルのリストを表示します。 すべての CSR ファイルはタイムスタンプされます。
ステップ 4	古い LSC 証明書の削除	古い LSC 証明書をシステムから削除します。

古い LSC レポートの実行

次の手順を使用して、古い LSC レポートを Cisco Unified レポートから実行します。 古い LSCs は、エンドポイント CSR への応答として生成された証明書ですが、古くなった LSCS がインストールされる前に新しい CSR が生成されたため、インストールされませんでした。

（注） また、パブリッシャーノードで `utils capf stale-lsc list` CLI コマンドを実行することによって、古い LSC 証明書のリストを取得することもできます。

手順

ステップ 1 Cisco Unified Reporting から **[System Reports]** をクリックします。

ステップ 2 左側のナビゲーションバーで、[**古い LSCs**] を選択します。

ステップ 3 **[新規レポートの生成]** をクリックします。

CAPF 経由の LSC 生成

CAPF を設定した後、電話機に設定されている認証文字列を追加します。 キーと証明書の交換は、電話機と CAPF の間で行われます。次のような場合があります。

- 電話機は、設定された認証方法を使用して CAPF に対して自身を認証します。
- 電話機は公開/秘密キー ペアを生成します。

- 電話機は、署名されたメッセージの中で、公開キーを CAPF に転送します。
- 秘密キーは電話に残り、外部に公開されることはありません。
- 証明書はCAPFによって署名され、署名付きメッセージによって電話に送り返されます。

（注） 電話のユーザが証明書操作の中断や、電話の動作ステータスの確認を実行できることに注意してください。

（注） キー生成の優先順位を低く設定すると、処理中に電話機を動作させることができます。証明書生成中にも電話は正常に機能しますが、TLS トラフィックが増加することで、電話での通話の処理に最小限の中断が発生する可能性があります。たとえば、インストールの最後に証明書がフラッシュに書き込まれると、音声信号が発生することがあります。

保留中の CSR リストの表示

保留中のCAPF CSR ファイルのリストを表示するには、この手順を使用します。すべてのCSR ファイルはタイムスタンプされます。

手順

ステップ 1 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。

ステップ 2 `utils core active list` CLI コマンドを実行します。
保留中の CSR ファイルのタイムスタンプリストが表示されます。

古い LSC 証明書の削除

古い LSC 証明書をシステムから削除するには、次の手順を使用します。

手順

ステップ 1 発行者ノードにログインするには、コマンドラインインターフェイスを使用します。

ステップ 2 `[utils capf state-lsc delete all` CLI コマンド] を実行します。
古い LSC 証明書はすべてシステムから削除されます。

CAPF システムの相互作用

表 *22 : CAPF* システム インタラクション

機能	データのやり取り
認証文字列（Authentication String）	CAPF認証方法で操作を行った後、電話に同じ認証文字列を入力しないと、操作は失敗します。 TFTP Encrypted Configuration エンタープライズ パラメータが有効で、認証文字列の入力に失敗した場合、一致する認証文字列が電話機に入力されるまで電話機に障害が発生し、回復しない可能性があります。
クラスタ サーバ クレデンシャル	Unified Communications Manager クラスタ内のすべてのサーバーは、CAPF がクラスタ内のすべてのサーバを認証できるように、同じ管理者のユーザ名とパスワードを使用する必要があります
セキュアな電話機の移行	セキュアな電話が別のクラスタに移動した場合、クラスタ Unified Communications Manager はその電話から送信された LSC 証明書を信頼しません。これは、その電話が別の CAPF により発行され、その証明書が CTL ファイルに含まれていないためです。 既存の CTL ファイルを削除して、セキュア電話を登録できるようにします。 その後、[インストール/アップグレード] オプションを使用して、新しい CAPF を持つ新しい LSC 証明書をインストールし、新しい CTL ファイルに対して電話をリセットします (または MIC を使用します)。 **[電話機の設定（Phone Configuration）]** ウィンドウの [CAPF] セクションにある **[削除（Delete）]** オプションを使用して、電話を移動する前に既存の LSC を削除します。
Cisco Unified IP Phones 6900、7900、8900、および 9900 シリーズ	Cisco Unified IP 電話の 6900、7900、8900、9900 シリーズをアップグレードして、LSC を使用して Unified Communications Manager への TLS 接続し、そして、 Unified Communications Manager トラストストアから MIC ルート証明書を削除することをお勧めします。互換性の問題を避けるためです。 MIC を使って Unified Communications Manager への TLS 接続を行う電話モデルでは、登録ができない場合があります。 管理者は次の MIC ルート証明書を Unified Communications Manager 信頼ストアから削除する必要があります: • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048

機能	データのやり取り
停電	以下の情報は、通信障害や電源障害の発生時に適用されます。 • 電話機に証明書をインストールしている間に通信障害が発生すると、電話機は証明書の取得を 30 秒間隔で 3 回試みます。 これらの値を構成することはできません。 • 電話が CAPF でセッションを試みている間に停電が発生した場合、電話はフラッシュに保存されている認証モードを使用します。 電話が TFTP サーバから新しい構成ファイルをロードできない場合、システムはフラッシュの値をクリアします。
証明書の暗号化	Unified Communications Manager リリース 11.5 (1) SU1 から始まり、CAPF サービスが発行するすべての LSC 証明書に SHA-256 アルゴリズムにより署名されます。 そのため、IP 電話 7900/8900/9900 シリーズのモデルは、SHA-256 署名済み LSC 証明書と外部 SHA2 アイデンティティ証明書 (Tomcat、 Unified Communications Manager、CAPF、TVS など) をサポートしています。 署名の検証が必要な、その他の暗号化の操作では、SHA-1 のみがサポートされます。 （注） ソフトウェアメンテナンス終了または製品寿命終了の電話モデルについては、11.5(1) SU1 リリース Unified Communications Manager 前のリリースを使用することをおすすめします。

7942 および 7962 電話機を含む CAPF の例

CAPFがユーザーまたは Cisco Unified IP 電話 が電話をリセットしたときに、7962および7942とどのように対話するかを検討してください。 Unified Communications Manager

（注） 例では、電話にLSCが存在せず、CAPF認証モードで **既存の証明書** を選択すると、CAPF証明書の操作が失敗します。

例：非セキュア デバイス セキュリティ モード

この例では、[Device Security Mode] を **[Nonsecure]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[By Existing Certificate (Precedence...)]** に設定した後、電話がリセットされます。 リセットした電話は直ちにプライマリ Unified Communications Manager に登録され、設定ファイルを受信します。 その後、電話によって LSC をダウンロードするための CAPF セッションが自動的に開始されます。 電話にダウンロードされた LSC がインストールされたら、[デバイス セキュリティ モード] を [認証済み] または [暗号化済み] に設定します。

例：認証済み/暗号化済みデバイス セキュリティ モード

この例では、**[Device Security Mode]** を **[Authenticated]** または **[Encrypted]** に設定し、[CAPF Authentication Mode] を **[By Null String]** または **[By Existing Certificate (Precedence...)]** に設定した後、電話がリセットされます。 CAPF セッションが終了し、電話に LSC がインストールされるまで、電話はプライマリ Unified Communications Manager に登録されません。 セッションが終了すると、電話が登録され、直ちに認証済みまたは暗号化済みモードで動作します。

この例では **認証文字列により** 設定することはできません。電話が CAPF サーバに自動的に接続しないためです。 電話に有効な LSC がない場合、登録は失敗します。

IPv6 アドレッシングとの CAPF のインタラクション

CAPF は、IPv4、IPv6、またはその両方のタイプのアドレスを使用する電話に対し、証明書の発行とアップグレードを実行できます。 IPv6 アドレスを使用して SCCP を実行している電話用の証明書を発行またはアップグレードするには、 **IPv6を有効にする** サービスパラメータを **True** に設定します。 Cisco Unified Communications Manager Administration

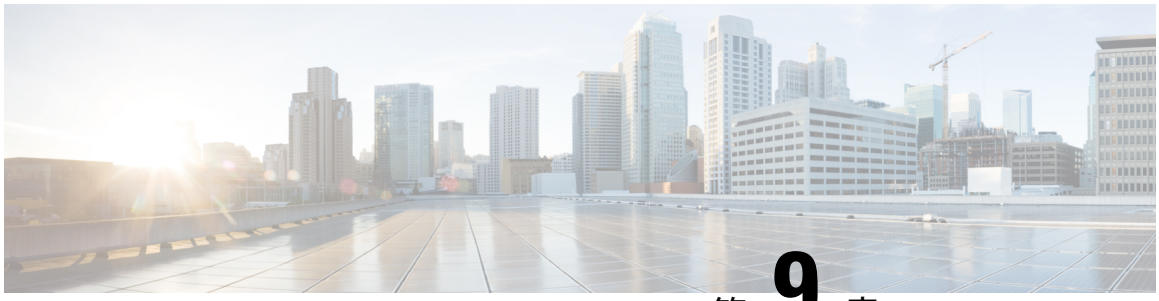
CAPF は、 **IPv6 を有効にする** エンタープライズパラメータの構成を使用して、電話への証明書を発行またはアップグレードします。 エンタープライズパラメータが **False** の場合、CAPF は IPv6 アドレスを使用する電話からの接続を無視/拒否し、電話は証明書を受け取りません。

IPv4、IPv6、またはその両方のタイプのアドレスを使用する電話から CAPF への接続方法について、次の表で説明します。

表 *23 : IPv6* または *IPv4* 電話から *CAPF* への接続方法

電話の IP モード	電話の IP アドレス	CAPF IP アドレス	電話から CAPF への接続方法
2 スタック	IPv4 と IPv6 が利用可能	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。 電話が IPv6 アドレス経由で接続できない場合、IPv4 アドレスを使用して接続を試みます。
2 スタック	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv6	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。 試行に失敗すると、電話は IPv4 アドレスを使用して CAPF に接続します。

電話の IP モード	電話の IP アドレス	CAPF IP アドレス	電話から CAPF への接続方法
2 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4 と IPv6 が利用可能	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
2 スタック	IPv4 と IPv6 が利用可能	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
2 スタック	IPv4	IPv6	電話が CAPF に接続できません。
2 スタック	IPv6	IPv4	電話が CAPF に接続できません。
2 スタック	IPv6	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv4、IPv6	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv6 スタック	IPv6	IPv4、IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv4	電話は IPv4 アドレスを使用して CAPF に接続します。
IPv4 スタック	IPv4	IPv6	電話が CAPF に接続できません。
IPv6 スタック	IPv6	IPv6	電話は IPv6 アドレスを使用して CAPF に接続します。
IPv6 スタック	IPv6	IPv4	電話が CAPF に接続できません。



第 9 章

TFTP 暗号化

- TFTP 暗号化構成ファイルの概要 （123 ページ）
- 電話設定ファイルの暗号化タスク フロー （125 ページ）
- TFTP 暗号化構成ファイルを無効にする （129 ページ）

TFTP 暗号化構成ファイルの概要

TFTP 設定は、登録プロセス中に電話機が TFTP サーバからダウンロードする設定ファイルを暗号化することにより、デバイス登録中のデータを保護します。 このファイルには、ユーザ名、パスワード、IP アドレス、ポートの詳細、電話の SSH 資格情報などの機密情報が含まれています。 この機能が構成されていない場合、構成ファイルはクリアテキストで送信されます。 この機能を展開することで、登録プロセス中に攻撃者がこの情報を傍受することはできません。 この情報は暗号化されず、クリアテキストで送信されます。 そのため、データを保護するために TFTP 設定ファイルを暗号化することを推奨します。

警告 SIP 電話のダイジェスト認証オプションを有効にして、TFTP 暗号化構成オプションを無効にしている場合、ダイジェスト認証情報はクリアテキストで送信されます。

TFTP 構成後、TFTP サーバは次のことを行います。

- ディスク上のすべてのクリアテキスト構成ファイルを削除します
- 構成ファイルの暗号化バージョンを生成します。

電話が暗号化された電話構成ファイルをサポートし、電話構成ファイルの暗号化のタスクを実行した場合、電話は暗号化バージョンの構成ファイルを要求します。

一部の電話は暗号化された電話構成ファイルをサポートしていません。 電話のモデルとプロトコルによって、システムが構成ファイルを暗号化するために使用する方法が決まります。 暗号化された構成ファイルをサポートする機能とファームウェアのロード Unified Communications Managerに依存する、サポートされている方法です。 電話ファームウェアのロードを、暗号化された構成ファイルをサポートしないバージョンにダウングレードすると、TFTP サーバは最

小限の構成設定を提供する暗号化されていない構成ファイルを提供します。その結果、電話が期待通りに動作しない可能性があります。

暗号化キーの配布

キー情報のプライバシーを確実に維持するために、暗号化された電話設定ファイルに関連するタスクはセキュアな環境で実行することを推奨します。

Unified Communications Manager は次のメソッドをサポートしています

- 手動キー配布。
- 電話の公開鍵による対称鍵暗号化。

手動鍵配布および電話の公開鍵を使用した対称鍵暗号化の設定情報は、**Cisco Unified CM Administration** ユーザーインターフェイスで TFTP 暗号化設定オプションを有効にしたことを前提としています。

TFTP 暗号化構成ファイルのヒント

TFTP 暗号化構成ファイルを有効にして、電話ダウンロードの機密データを保護することをお勧めします。 PKI 機能のない電話の場合は、Unified Communications Manager Administration と電話で対称キーを設定する必要があります。 電話または Unified Communications Manager から対称キーが見つからない、またはTFTP暗号化構成ファイルが設定されているときに不一致が発生する場合、電話は登録できません。

Unified Communications Managerで暗号化構成ファイルを構成する場合は、次の情報を考慮してください:

- 暗号化構成ファイルに対応する電話のみが **電話セキュリティプロファイル設定** ページの **TFTP暗号化設定** チェックボックスを表示します。 Cisco Unified IP 電話7800、7942、および 7962 (SCCP のみ) の暗号化構成ファイルを構成することはできません。これらの電話はダウンロードされた構成ファイルで機密データを受信しないためです。
- **TFTP 暗号化設定** チェックボックスはデフォルトでオフになっています。 このデフォルト設定を適用すると、電話に非セキュア プロファイル、ダイジェスト クレデンシャル、およびセキュア パスワードがクリアテキストで送信されます。
- 公開鍵暗号化を使用するCisco Unified IP電話では、暗号化された構成ファイルを有効にするために、端末セキュリティモードを認証済みまたは暗号化済みに設定する必要はありません。 Unified Communications Manager は登録時に公開鍵をダウンロードするCAPFプロセスを使用します。 Unified Communications Manager
- 使用中の環境が安全であることがわかっている場合、またはPKIが有効になっていない電話に対称キーを手動で構成することを避けるために、暗号化されていない構成ファイルを電話にダウンロードすることを選択できます。 ただし、この方法の使用はお勧めしません。
- Cisco Unified IP 電話7800、7942、7962 (SIP のみ) については、ダイジェスト証明書を電話機に送信する方法を提供します。暗号化設定を使用するより簡単ですが、安全性は劣りま

す。 Unified Communications Manager [構成ファイルからダイジェスト資格情報を除外する] 設定を使用するこの方法は、最初に対称キーを構成して電話に入力する必要がないため、ダイジェスト資格情報を初期化する場合に便利です。 この方法では、ダイジェスト クレデンシャルを非暗号化設定ファイルで電話機に送信します。 資格情報を電話に入力したら、**[電話セキュリティプロファイルの設定（Phone Security Profile Configuration）]** ページで、**[TFTP 暗号化設定（TFTP Encrypted Config）]** オプションを無効にしてから、**[設定ファイルからダイジェスト証明書を除外する（Exclude Digest Credential in Configuration File）]** オプションを有効にすることをお勧めします。 これにより、今後のダウンロードからダイジェスト認証情報が除外されます。

- ダイジェスト クレデンシャルがこれらの電話に存在し、受信ファイルにダイジェスト クレデンシャルが含まれていない場合、既存のクレデンシャルがそのまま残ります。 ダイジェストの資格情報は、電話が工場出荷時の設定にリセットされるか、新しい資格情報(空白を含む)が受信されるまで、そのまま残ります。 電話機またはエンドユーザーのダイジェスト資格情報を変更する場合は、対応する **[電話機セキュリティプロファイル情報（Phone Security Profile Information）]** ページの 設定ファイルから **[ダイジェスト資格情報を除外する（Exclude Digest Credential in Configuration File）]** を一時的に無効にして、新しいダイジェスト資格情報を電話にダウンロードします。

電話設定ファイルの暗号化タスク フロー

TFTP 構成ファイルの暗号化をセットアップするには、クラスタ内の電話が手動キー暗号化と公開キー暗号化をサポートしていることを確認し、電話が SHA-1 および SHA-512 をサポートしていることを確認したら、次のタスクを完了します。

（注） クラスター全体で SHA-512 を有効にした場合で、電話がサポートしていない場合、これらの電話は機能しません。

手順

	コマンドまたはアクション	目的
ステップ 1	TFTP暗号化を有効にする （126ページ）	電話の TFTP 構成ファイル オプションを有効にします。 電話セキュリティ プロファイルでこのオプションを有効にできます。
ステップ 2	SHA-512 署名アルゴリズムの設定 （126ページ）	TFTP ファイル暗号化が有効な場合、デフォルトで SHA-1 が署名アルゴリズムとして構成されます。 この手順でシステムを更新し、より強力な SHA-512 アルゴリズムを使用します。

	コマンドまたはアクション	目的
ステップ 3	LSC または MIC 証明書のインストールを確認する （127 ページ）	公開キーを使用する電話の場合、証明書のインストールを確認します。
ステップ 4	CTL ファイルの更新 （128 ページ）	TFTP 構成ファイルの更新が完了したら、CTL ファイルを再生成します。
ステップ 5	サービスの再起動 （128 ページ）	Cisco CallManager および Cisco TFTP サービスを再起動してください。
ステップ 6	電話をリセット （129 ページ）	暗号化 TFTP 構成ファイルの更新が完了したら、電話をリセットします。

TFTP 暗号化を有効にする

特定の電話モデルの電話セキュリティ プロファイル内でこの TFTP を有効にできます。 この手順を実行して TFTP サーバからダウンロードしたファイルの TFTP 暗号化を有効にします。

手順

ステップ 1 Cisco Unified CM Administration から、以下を選択します。**システム** > **セキュリティ** > **電話セキュリティ プロファイル**。

ステップ 2 **検索する** をクリックし、電話セキュリティ プロファイルを選択します。

ステップ 3 **TFTP 暗号化設定** チェックボックスを選択します。チェックしてください。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 クラスタで使用される他の電話セキュリティ プロファイルに対して、これらの手順を繰り返します。

（注）
電話構成ファイルの暗号化を無効にするには、 **の電話セキュリティ プロファイルの** TFTP Encrypted Config Cisco Unified Communications Manager Administration チェックボックスを解除し、その変更を保存する必要があります。

SHA-512 署名アルゴリズムの設定

SHA-1 は TFTP ファイル署名のデフォルトのアルゴリズムです。 以下のオプションの手順を使用してシステムをアップグレードし、デジタル署名などの TFTP 構成ファイルにより強力な SHA-512 アルゴリズムを使用できます。

（注） お使いの電話が SHA-512 をサポートしていることを確認してください。 そうでない場合、システムを更新した後に電話が機能しません。

手順

ステップ 1 Cisco Unified CM Administration から、以下を選択します。**システム** > **エンタープライズパラメータ**。

ステップ 2 [**セキュリティパラメータ**] ペインに移動します。

ステップ 3 **TFTP ファイル署名アルゴリズム** ドロップダウンリストから、 **SHA-512 を選択します**。

ステップ 4 **[保存（Save）]** をクリックします。

ポップアップ ウィンドウにリストされている影響を受けるサービスを再起動して、手順を完了します。

LSC または MIC 証明書のインストールを確認する

公開キーを使用する電話の場合、証明書のインストールを確認します。

（注） この手順は、PKI 暗号化を使用する Cisco Unified IP 電話に適用されます。 お使いの電話が PKI 暗号化をサポートしているかどうかを判断するには、「暗号化構成ファイルをサポートしている電話モデル」セクションを参照してください。

以下の手順は、電話が Unified Communications Manager データベースに存在し、TFTP 暗号化設定パラメータが Unified Communications Manager で有効になっていることを前提としています。

手順

ステップ 1 製造元でインストールされた証明書 (MIC) またはローカルで有効な証明書 (LSC) が電話に存在することを確認します。

ステップ 2 Cisco Unified CM Administration から、**[デバイス] > [電話機]** を選択します。
電話のリストが表示されます。

ステップ 3 **端末名**をクリックします。
[電話設定] ページが表示されます。

ヒント

[電話機の設定（Phone Configuration）] ページの [CAPF 設定（CAPF settings）] セクションで **[トラブルシューティング（Troubleshoot）]** オプションを選択し、Unified Communications Manager の電話に LSC または MIC が存在するかどうかを確認します。 証明書が電話に存在しない場合、[削除] および [トラブルシューティング] オプションは表示されません。

ヒント
また、電話機のセキュリティ設定をチェックすることで、電話機に LSC または MIC が存在することを確認できます。 詳細については、このバージョンの Cisco Unified IP 電話をサポートする Unified Communications Managerの管理ガイドを参照してください。

ステップ 4 証明書が存在しない場合は、[**電話設定**] ウィンドウでCAPF機能を使用してLSCをインストールします。 LSC のインストール方法については、認証局プロキシ機能に関連するトピックを参照してください。

ステップ 5 CAPF 設定が完了したら、**[保存（Save）]** をクリックします。

ステップ 6 [リセット（**Reset**）] をクリックします。
電話機は、リセット後に TFTP サーバに暗号化された設定ファイルを要求します。

CTL ファイルの更新

Unified Communications Manager で変更を行ったら、CTL ファイルを更新します。 TFTP ファイル暗号化を有効にしたため、CTL ファイルを再生成する必要があります。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 パブリッシャノードで、 **utils ctl update CTLfile** コマンドを実行します。

サービスの再起動

暗号化 TFTP 構成ファイルの更新が完了したら、変更を有効にするために Cisco TFTP および Cisco CallManager サービスを再起動してください。

手順

ステップ 1 [Cisco Unified Serviceability] から、以下を選択します。**ツール** > **コントロールセンター – 機能サービス**。

ステップ 2 次の 2 つのサービスを選択します。

- Cisco CallManager
- Cisco TFTP

ステップ 3 **[再起動（Restart）]** をクリックします。。

電話をリセット

暗号化 TFTP 構成ファイルの更新がすべて完了したら、必ず電話をリセットしてください。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[電話機（Phones）]** を選択します。

ステップ 2 **[検索（Find）]** をクリックします。

ステップ 3 [**すべて選択**] をクリックします。

ステップ 4 [選択したアイテムのリセット（Reset Selected）] をクリックします。

TFTP 暗号化構成ファイルを無効にする

警告 SIP を実行している電話でダイジェスト認証が **True** で、TFTP 暗号化構成設定が **False** の場合、ダイジェスト資格情報が平文で送信される場合があります。

設定の更新後、電話の暗号化キーは Unified Communications Managerデータベースに残ります。

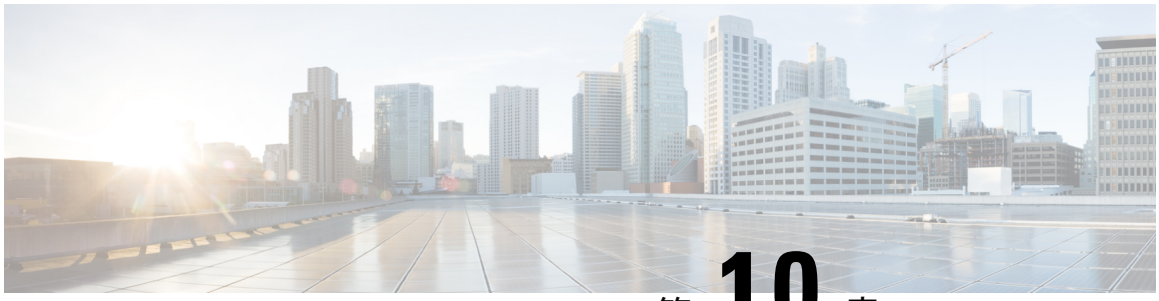
Cisco Unified IP 電話 の 7911G、7931G（SCCP のみ）、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、および 7975G が暗号化構成設定が **[いいえ（False）]** に更新されると、暗号化されたファイル（.enc.sgn ファイル）をリクエストし、電話は暗号化されていない、署名されたファイル（.sgn ファイル）をリクエストします。

Cisco Unified IP 電話が SCCP および SIP で実行されている場合、暗号化構成設定が **False** に更新されたら暗号化ファイルを要求します。 電話の GUI から対称キーを削除して、次に電話がリセットされたときに、暗号化されていない構成ファイルが要求されるようにします。

- Cisco Unified IP 電話s SCCP 実行: 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7925G, 7925G-EX, 7926G, 7931G, 7941G, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7975G, 8941, 8945.
- SIP で動作する Cisco Unified IP 電話：6901、6911、6921、6941、6945、6961、7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G-GE、7962G、7965G、7975G、8941、8945、8961、9971、7811、78321、7841、7861、7832、8811、8841、8845、8851、8851NR、8861、8865、8865NE、8821、8831、8832、8832NR。

手順

	コマンドまたはアクション	目的
ステップ 1	電話設定ファイルの暗号化を無効にするには、その電話に関連付けられている電話セキュリティプロファイルの [**TFTP 暗号化設定**] チェックボックスのチェックを解除します。	
ステップ 2	Cisco Unified IP 電話7942 および 7962 (SIP のみ) では、電話スクリーンに表示される対称キーの値として 32 バイトの 0 を入力して、暗号化を無効にします。	
ステップ 3	Cisco Unified IP 電話s (SIP のみ) では、電話スクリーンで対称キーを削除して暗号化を無効にします。	これらのタスクの実行方法については、お使いの電話モデルに対応する電話管理ガイドを参照してください。



第 10 章

電話機のセキュリティ

- 電話のセキュリティの概要 （131 ページ）
- 電話セキュリティ プロファイル （143 ページ）
- SIP 電話のダイジェスト認証の概要 （165 ページ）

電話のセキュリティの概要

インストール時、Unified Communications Manager は非セキュアモードで起動します。 Unified Communications Manager のインストール後に電話を起動すると、すべての端末が非セキュア Unified Communications Manager として登録されます。

Unified Communications Manager 4.0(1) 以降のリリースからアップグレード後、電話はアップグレード前に有効にしたデバイスセキュリティモードで起動します。すべてのデバイスは、選択したセキュリティモードを使用して登録されます。

Unified Communications Manager インストールにより、 Unified Communications Manager および TFTP サーバ上に自己署名証明書が作成されます。 自己署名証明書の代わりに、 Unified Communications Manager サードパーティの CA 署名付き証明書を使用することもできます。 認証を設定すると、 Unified Communications Manager はその証明書を使ってサポートされている Cisco Unified IP Phone で認証を行います。 Unified Communications Manager と TFTP サーバ上に証明書が存在する場合、 Unified Communications Manager が各アップグレード時に証明書を再発行することはありません。 Unified Communications Manager CLI コマンド **util ctl update CTLFile** を新しい証明書エントリで使用して、ctl ファイルを更新する必要があります。

ヒント サポートされていない、または安全ではないシナリオに関する情報については、対話と制限に関連するトピックを参照してください。

Unified Communications Manager は、デバイス レベルで認証と暗号化のステータスを管理します。 通話に関連するすべてのデバイスがセキュアとして登録されている場合、通話ステータスはセキュアとして登録されます。 1 つのデバイスが非セキュアとして登録されると、発信者または受信者の電話がセキュアとして登録されている場合でも、通話は非セキュアとして登録されます。

ユーザーが Cisco Extension Mobility を使用している場合、Unified Communications Manager はデバイスの認証と暗号化のステータスを保持します。Unified Communications Manager は共有ラインが設定されている場合も、デバイスの認証と暗号化のステータスを保持します。

ヒント　暗号化された Cisco IP 電話の共有回線を設定する場合、回線を共有するすべてのデバイスで暗号化を設定します。つまり、暗号化をサポートするセキュリティプロファイルを適用することで、すべてのデバイスのデバイスセキュリティモードを暗号化に設定します。

電話セキュリティ強化の概要

このセクションでは、Gratuitous ARP の無効化、ウェブアクセスの無効化、PC 音声 VLAN アクセスの無効化、アクセスの無効化、PC ポートの無効化の設定など、電話のハードニングの動作の概要について説明します。

以下のオプション設定は、Cisco IP 電話への接続を強化するために使用されます。**[電話機の設定（Phone Configuration）]** ウィンドウの [プロダクト固有の設定（Product-Specific Configuration Layout）] に、これらの設定が表示されます。

これらの設定は、一連の電話、またはすべての企業全体の電話に適用する場合、**[共通の電話プロファイルの設定（Common Phone Profile Configuration）]** ウィンドウと **[企業の電話機の設定（Enterprise Phone Configuration）]** ウィンドウにも表示されます。

表 *24 :* 電話強化の動作

電話強化の動作	説明	
Gratuitous ARP の無効化	デフォルトでは、Cisco Unified IP Phone は、Gratuitous ARP パケットを受け付けます。 デバイスが使用する Gratuitous ARP パケットは、ネットワーク上のデバイスの存在を通知します。 しかし、攻撃者はこれらのパケットを使用して、有効なネットワーク デバイスになりすますことができます。たとえば、攻撃者はデフォルトルーターを装ったパケットを送信する可能性があります。無効にする場合は、[**電話設定**] ウィンドウで、Gratuitous ARP を無効にすることができます。 （注） この機能を無効にしても、電話がデフォルトルーターを識別することはできます。	

電話強化の動作	説明	
ウェブアクセスの無効化	電話のウェブサーバ機能を無効にすると、統計と設定情報を提供する電話の内部ウェブページへのアクセスがブロックされます。 CiscoQuality Report Tool などの機能は、電話のウェブページにアクセスしないと正しく機能しません。 ウェブ サーバを無効にすると、Web アクセスに依存する CiscoWorks などの Serviceability アプリケーションにも影響します。 ウェブ サービスが無効かどうかを判断するために、電話はサービスが無効か有効かを示す構成ファイルのパラメータを解析します。 ウェブ サービスが無効になっている場合、電話機はモニタリングの目的で HTTP ポート 80 を開かず、電話機の内部ウェブページへのアクセスをブロックします。	
PC 音声 VLAN アクセスの無効化	デフォルトでは、Cisco IP Phone はスイッチポート（アップストリームスイッチに向かうポート）で受信したすべてのパケットを PC ポートに転送します。 [電話の設定] ウィンドウで [PC 音声 VLAN アクセス] 設定を無効にした場合、音声 VLAN 機能を使用する PC ポートから受信したパケットはドロップされます。 Cisco IP Phone はこの機能を異なる方法で使用します。 • Cisco Unified IP Phone 7942 および 7962 は、PC ポート内外で、音声 VLAN でタグ付けされたパケットをドロップします。	

電話強化の動作	説明	
アクセス無効に設定する	Cisco IP Phone の [アプリケーション] ボタンを押すと、既定では電話設定情報を含む様々な情報にアクセスすることができます。 [電話の設定] ウィンドウの [設定アクセス] パラメータを無効にすると、通常、電話機の [アプリケーション] ボタンを押したときに表示されるすべてのオプションへのアクセスが禁止されます。たとえば、[コントラスト]、[呼び出し音のタイプ]、[ネットワーク設定]、[モデル情報]、[ステータス] 設定などです。 Unified Communications Manager Administration で設定が無効になっている場合、上記の設定は電話では表示されません。この設定を無効にすると、電話ユーザは [音量] ボタンに関連する設定を保存できません。例えば、ユーザはボリュームを保存できません。 この設定を無効にすると、電話の現在の [コントラスト]、[呼び出し音のタイプ]、[ネットワーク設定]、[モデル情報]、[ステータス]、[音量] の各設定が自動的に保存されます。 これらの電話設定を変更するには、Unified Communications Manager Administration で [アクセス設定（Setting Access）] 設定を有効にする必要があります。	

電話強化の動作	説明	
PC ポートの無効化	Unified Communications Manager は、PC ポートを持つすべての Cisco IP Phone の PC ポートをデフォルトで有効にします。[電話の設定] ウィンドウで [PC ポート] 設定を無効にすることができます。 ロビーや会議室の電話では PC ポートを無効にすると便利です。 （注） PC ポートは一部の電話機で利用でき、ユーザはコンピュータを電話機に接続することができます。 この接続方法では、ユーザが必要とする LAN ポートは 1 つだけです。	

電話セキュリティ強化のセットアップ

電話強化は、接続を強化するために電話に適用できるオプションの設定で構成されています。設定は、次の 3 つの構成ウィンドウのいずれかを使用して適用できます。

- 電話設定 - [**電話設定**] ウィンドウを使用して、個々の電話に設定を適用します。
- 共通の電話プロファイル - **[共通の電話プロファイル**] ウィンドウを使用して、このプロファイルを使用するすべての電話に設定を適用します。
- 企業の電話: すべての企業の電話に設定を適用するには、[**企業の電話**] ウィンドウを使用します

（注） これらの各ウィンドウで矛盾する設定が表示された場合、電話が正しい設定を判断するために使用する優先順位は次のとおりです。1) 電話の設定、2) 共通の電話プロファイル、3) 企業の電話

電話セキュリティ強化をセットアップするには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから **端末** > **電話**を選択します。

ステップ 2 電話を検索する基準を指定し、[**検索**] をクリックすると、すべての電話の一覧が表示されます。

ステップ 3 デバイス名をクリックします。

ステップ 4 以下の製品固有のパラメータを特定します。

a) PC Port
b) アクセスの設定
c) Gratuitous ARP
d) PC の音声 VLAN へのアクセス（PC Voice VLAN Access）
e) Web アクセス（Web Access）

ヒント
これらの設定に関する情報を確認するには、[**電話設定**] ウィンドウのパラメータのとなりにあるヘルプアイコンをクリックしてください。

ステップ 5 無効にしたい各パラメータのドロップダウンリストから [**無効**] を選択します。 スピーカーフォンまたはスピーカーフォンとヘッドセットを無効にするには、対応するチェックボックスをチェックします。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 [**リセット（Reset）**] をクリックします。

信頼できるデバイス

Unified Communications Manager により、Cisco IP 電話の電話モデルごとにセキュリティアイコンを有効にできます。[セキュリティ]アイコンは、通話が安全かどうか、および接続されたデバイスが信頼できるかどうかを示します。

信頼されたデバイスは、信頼された接続のための Cisco セキュリティ基準に合格した Cisco デバイスまたはサードパーティ デバイスを表します。 これには、シグナリング/メディア暗号化、プラットフォーム強化、保証が含まれますが、これらに限定されるものではありません。デバイスが信頼されている場合、サポートされているデバイスで[セキュリティ]アイコンが表示され、セキュアなトーンが鳴ります。また、デバイスは、セキュアなコールに関連する他の機能またはインジケータを提供する場合があります。

Unified Communications Manager は、システムに追加するときに、デバイスが信頼できるかどうかを判断します。 セキュリティアイコンは情報提供のみを目的として表示され、管理者が直接設定することはできません。

Unified Communications Manager は、Unified Communications Manager Administration にアイコンとメッセージを表示して、ゲートウェイが信頼できるかどうかを示します。

このセクションでは、Cisco IP 電話および Unified Communications Manager Administration の両方での、信頼できる端末のセキュリティアイコンの動作について説明します。

Cisco Unified Communications Manager Administration

Unified Communications Manager Administration の次のウィンドウは、デバイスが信頼できるかどうかを示します:

[ゲートウェイの設定（Gateway Configuration）]

各ゲートウェイタイプに対して、[ゲートウェイ設定] ウィンドウ (**端末** > **ゲートウェイ**) には、次のいずれかが表示されます。 **端末は信頼されています** または **端末は信頼されていません**と対応するアイコンが表示されます。

デバイスが信頼済みであるかどうかは、デバイス タイプに基づいて判別されます。 デバイスが信頼済みであるかどうかは設定できません。

電話機設定

各電話デバイスタイプに対して、[電話機設定（Phone Configuration）] ウィンドウ（**[デバイス（Device）]** > **[電話機（Phone）]**）には、対応するアイコンと共に、**[デバイスは信頼済み（Device is trusted）]** または **[デバイスは信頼されていない（Device is not trusted）]** のいずれかが表示されます。

デバイスが信頼済みであるかどうかは、デバイス タイプに基づいて判別されます。 デバイスが信頼済みであるかどうかは設定できません。

呼び出されたデバイスの信頼性の判断基準

ユーザが発信するデバイスのタイプは、電話に表示されるセキュリティ アイコンに影響します。 システムは次の 3 つの基準を考慮して、通話がセキュアかどうかを判断します。

- 通話中のすべてのデバイスは信頼されていますか?
- シグナリングはセキュアですか（認証および暗号化されていますか）?
- メディアはセキュアですか?

サポートされている Cisco Unified IP 電話 がロックセキュリティアイコンを表示するようにするには、3 つの条件すべてを満たす必要があることに注意してください。 信頼されていないデバイスを含む通話の場合、シグナリングとメディアセキュリティに関係なく、通話の全体的なステータスは不安全なままになり、電話はロックアイコンを表示しません。 たとえば、電話会議に信頼されていないデバイスが含まれる場合、システムはそのコール レッグおよび電話会議自体がセキュアではないと見なします。

電話機モデルのサポート

Unified Communications Manager のセキュリティをサポートする電話モデルには、Secure Cisco phonesとSecure Preferred Vendor phonesの 2 つのカテゴリがあります。 Secure Cisco phonesには、製造元でインストールされた証明書 (MIC) がプリインストールされており、認証局プロキシ機能 (CAPF) を使用したローカルで有効な証明書 (LSC) の自動生成と交換をサポートしています。 Secure Cisco phonesは、追加の証明書管理なしで MIC を使用して Cisco Unified CM に登録

できます。 セキュリティを強化するために、CAPF を使用して LSC を作成し、電話機にインストールできます。 詳細については、電話セキュリティのセットアップと設定に関するトピックを参照してください。

安全な優先ベンダーの電話には MIC が事前にインストールされておらず、LSC を生成するための CAPF をサポートしていません。 セキュアな優先ベンダーの電話を Cisco Unified CM に接続するには、証明書がデバイスで提供されるか、デバイスによって生成される必要があります。 電話のサプライヤーは、電話の証明書を取得または生成する方法の詳細を提供する必要があります。 証明書を取得したら、OS管理の証明書管理インターフェースを使用して、Cisco Unified CM に証明書をアップロードする必要があります。 詳細については、優先ベンダーの SIP 電話セキュリティのセットアップに関するトピックを参照してください。

お使いの電話でサポートされているセキュリティ機能の一覧については、この Unified Communications Manager リリースに対応する電話管理およびユーザ用ドキュメント、またはお使いのファームウェアに対応するファームウェアのドキュメントを参照してください。

Cisco Unified Reporting を使って、対応している電話の一覧を表示することもできます。 Cisco Unified Reporting の使用方法の詳細については、『 Cisco Unified Reporting アドミニストレーションガイド』を参照してください。

電話セキュリティ設定の表示

セキュリティをサポートする電話で特定のセキュリティ関連の設定を構成および表示できます。たとえば、電話機にローカルで有効な証明書があるかどうか、または製造元でインストールされた証明書がインストールされているかどうかを確認できます。セキュリティメニューとアイコンの詳細については、『 *Cisco IP Phone* 管理者ガイド および *Cisco IP Phone* ユーザガイド』を参照してください。

Unified Communications Manager が通話を認証済みまたは暗号化済みに分類すると、アイコンが電話機に表示され、通話状態を示します。 また、 Unified Communications Manager が通話を認証済みまたは暗号化済みに分類するタイミングも決定します。

電話セキュリティのセットアップ

次の手順では、サポートされている電話のセキュリティを設定するタスクについて説明します。

手順

ステップ 1 まだ行っていない場合は、Cisco CTL Clientを設定し、Unified Communications Manager セキュリティモードが [混合モード（Mixed Mode）] になっていることを確認します。

ステップ 2 電話にローカルで有効な証明書 (LSC) または製造元でインストールされた証明書 (MIC) が含まれていない場合、認証局プロキシ 機能 (CAPF) を使用して LSC をインストールします。

ステップ 3 電話セキュリティ プロファイルを設定します。

ステップ 4 電話セキュリティ プロファイルを電話に適用します。

ステップ 5 ダイジェストクレデンシャルを設定した後、[電話の設定] ウィンドウから [ダイジェストユーザ] を選択します。

ステップ 6 Cisco Unified IP 電話 7962 または 7942（SIP のみ）で、[エンドユーザーの設定（End User Configuration）] ウィンドウで設定したダイジェスト認証のユーザー名とパスワード（ダイジェスト認証の資格情報）を入力します。

（注）
このドキュメントでは、ダイジェスト認証クレデンシャルを電話で入力する手順については説明していません。 このタスクの実行方法に関する情報は、お使いの電話モデルをサポートする『Cisco Unified Communications Manager アドミニストレーション ガイド』とこのバージョンの Unified Communications Manager を参照してください。

ステップ 7 電話がこの機能をサポートしている場合、電話設定ファイルを暗号化してください。

ステップ 8 電話のセキュリティを強化するには、電話設定を無効にしてください。

優先ベンダー SIP 電話セキュリティのセットアップ

安全な優先ベンダーの電話は、サードパーティ ベンダーによって製造された電話タイプですが、COP ファイルを介して Cisco Unified データベースにインストールされます。 Unified Communications Manager は、優先ベンダーの SIP 電話にセキュリティを提供します。 セキュリティをサポートするには、COP ファイルで優先ベンダーの SIP 電話に対してセキュリティ暗号化またはセキュリティ認証を有効にする必要があります。 これらの電話タイプは、[新しい電話の追加] ウィンドウのドロップダウン リストに表示されます。 すべての優先ベンダーの電話はダイジェスト認証をサポートしていますが、すべての優先ベンダーの電話が TLS セキュリティをサポートしているわけではありません。 セキュリティ機能は電話モデルに基づきます。 電話セキュリティプロファイルに [「端末セキュリティモード」] フィールドが含まれている場合、TLS セキュリティがサポートされます。

希望のベンダーの電話が TLS セキュリティをサポートしている場合、デバイスごとの証明書と共有証明書の 2 つのモードが可能です。 電話機のサプライヤーは、どのモードが電話機に適用できるか、および電話機の証明書を生成または取得するための手順を指定する必要があります。

優先ベンダー SIP 電話セキュリティ プロファイル デバイスごとの証明書のセットアップ

デバイスごとの証明書で優先ベンダーの SIP 電話セキュリティ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

ステップ 1 OS 管理の証明書管理インターフェイスを使用して、各電話の証明書をアップロードします。

ステップ 2 Cisco Unified CM Administration で、**[システム（System）] > [セキュリティ（Security）] > [電話セキュリティプロファイル（Phone Security Profile）]** の順に選択します。

ステップ 3 この電話のデバイスタイプに新しい電話セキュリティプロファイルを設定し、[**デバイスセキュリティモード**] ドロップダウンリストで **暗号化** または **認証**を選択します。

ステップ 4 CCMAdmin インターフェイスで新しい SIP 電話を設定するには、[**端末** > **電話** > **新規追加**] を選択します。

ステップ 5 [電話タイプ] を選択します。

ステップ 6 必須フィールドに入力します。

ステップ 7 [**デバイスセキュリティプロファイル**] ドロップダウンリストから、作成したプロファイルを選択します。

優先ベンダー SIP 電話セキュリティ プロファイルの共有証明書のセットアップ

共有証明書で指定ベンダーの SIP 電話セキュリティ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

ステップ 1 電話ベンダーからの指示を使用して、サブジェクト代替名 (SAN) 文字列で証明書を生成します。 SAN は DNS タイプである必要があります。 この手順で指定した SAN をメモします。 例えば、X509v3 の拡張の場合：

- X509v3 サブジェクト代替名
- DNS:AscomGroup01.acme.com

（注）
SAN は DNS タイプである必要があります。そうでない場合、セキュリティは有効になりません。

ステップ 2 OS 管理の証明書管理インターフェイスを使用して共有証明書をアップロードします。

ステップ 3 Cisco Unified CM Administration で、**[システム（System）]** > **[セキュリティ（Security）]** > **[電話セキュリティプロファイル（Phone Security Profile）]** の順に選択します。

ステップ 4 **[名前（Name）]**フィールドに、優先ベンダーから提供された証明書に記載されているサブジェクト代替名（SAN）を入力します。SANがない場合は、証明書名を入力します。

（注）
セキュリティプロファイルの名前は、証明書の SAN と正確に一致する必要があります。一致しない場合、セキュリティは有効になりません。

ステップ 5 **[デバイスのセキュリティモード（Device Security Mode）]** ドロップダウンメニューから、**[暗号化（Encrypted）]** または **[認証済み（Authenticated）]** を選択します。

ステップ 6 [トランスポートタイプ] ドロップダウンリストから、 **TLS** を選択します。

ステップ 7 CCMAdmin インターフェイスで新しい SIP 電話を設定するには、[**端末** > **電話** > **新規追加**] を選択します。

ステップ 8 [電話タイプ] を選択します。

ステップ 9 必須フィールドに入力します

ステップ 10 [**デバイスセキュリティプロファイル**] ドロップダウンリストから、作成したプロファイルを選択します。

あるクラスターから別のクラスターに電話を移行する

次の手順を使用して、電話を1つのクラスタから別のクラスタに移行します。 たとえば、クラスター 1 からクラスター 2 に。

手順

ステップ 1 Cisco Unified OS Administration のクラスタ 2 から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[検索（Find）]** をクリックします。

ステップ 3 証明書のリストから、ITLRecovery 証明書をクリックし、**[.PEM ファイルのダウンロード（Download .PEM File）]** または **[.DER ファイルのダウンロード（Download .DER File）]** のいずれかをクリックして、いずれかのファイル形式の証明書をコンピュータにダウンロードします。
証明書の詳細が表示されます。

ステップ 4 証明書のリストから、CallManager 証明書をクリックし、**[.PEM ファイルのダウンロード（Download .PEM File）]** または **[.DER ファイルのダウンロード（Download .DER File）]** のいずれかをクリックして、いずれかのファイル形式の証明書をコンピュータにダウンロードします。
証明書の詳細が表示されます。

ステップ 5 Cisco Unified OS Administration のクラスタ 1 から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。
[証明書の一覧（Certificate List）]ウィンドウが表示されます。

ステップ 6 **証明書チェーンのアップロード**をクリックして、ダウンロードした証明書をアップロードします。

ステップ 7 [証明書の目的（Certificate Purpose）] ドロップダウンリストで、[Phone-SAST-trust] を選択します。

ステップ 8 **[ファイルのアップロード（Upload File）]** フィールドについて、**[ファイルを選択（Choose File）]** をクリックし、ステップ 3 でダウンロードした ITLRecovery ファイルを参照し、**[ファイルをアップロード（Upload File）]** をクリックします。

アップロードされた ITLRecovery ファイルは、クラスタ 1 の **[証明書一覧（Certificate List）]** ウィンドウに **Phone-SAST-Trust** 証明書として表示されます。新しい ITL ファイルにクラスタ 2 の ITLRecovery 証明書がある場合は、コマンド `show itl` を実行します。

ステップ 9 クラスタ 1 の電話にローカルで有効な証明書 (LSC) がある場合、クラスタ 1 からの CAPF 証明書はクラスタ 2 の CAPF 信頼ストアにアップロードされる必要があります。

ステップ 10 （任意） この手順は、クラスターが混合モードの場合にのみ適用できます。 CLI で **utils ctl update CTLFile** コマンドを実行し、クラスター 1 で CTL ファイルを再生成します。

（注）
- `show ctl` CLI コマンドを実行して、クラスタ 2 の ITLRecovery 証明書と CallManager 証明書が、SASTの役割を持つ CTL ファイルに含まれていることを確認します。
- 電話が新しい CTL および ITL ファイルを受信したことを確認します。 更新された CTL ファイルには、クラスター 2 の ITLRecovery 証明書があります。

クラスタ 1 からクラスタ 2 に移行する電話は、クラスタ 2 の ITLRecovery 証明書を受け入れるようになります。

ステップ 11 1 つのクラスタから別のクラスタに電話を移行します。

電話のセキュリティ インタラクションと制限事項

このセクションでは、電話セキュリティのインタラクションと制限事項について説明します。

表 *25 :* 電話機のセキュリティインタラクションと制限事項

機能	連携動作と制限事項
証明書の暗号化	Unified Communications Manager 11.5 (1) SU1 リリース以降、CAPF サービスが発行するすべての LSC 証明書は SHA-256 アルゴリズムで署名されています。 そのため、 Cisco Unified IP 電話 7900 シリーズ、8900 シリーズ、9900 シリーズはSHA-256 署名済み LSC 証明書と外部 SHA2 アイデンティティ証明書 (Tomcat、CallManager、CAPF、TVS など) をサポートしています。 署名の検証が必要な、その他の暗号化の操作では、SHA-1 のみがサポートされます。 （注） ソフトウェアメンテナンスが終了またはサポートが終了した電話モデルを使用する場合は、Unified Communications Manager の 11.5(1)SU1 より前のリリースの使用を強くお勧めします。

電話セキュリティ プロファイル

Unified Communications Manager は、電話機の種類とプロトコルに関連するセキュリティ設定をセキュリティプロファイルにグループ化します。 そのため、この単一のセキュリティプロファイルを複数の電話に割り当てることができます。 セキュリティ関連の設定には、デバイス セキュリティ モード、ダイジェスト認証、および一部の CAPF 設定が含まれます。 インストール Unified Communications Manager では、自動登録用の事前定義された非セキュアなセキュリティプロファイルのセットが提供されます。

[**電話の構成**] ウィンドウでセキュリティプロファイルを選択することで、構成した設定を電話に適用できます。 電話のセキュリティ機能を有効にするには、デバイス タイプとプロトコルの新しいセキュリティ プロファイルを設定し、そのプロファイルを電話に適用する必要があります。 選択した端末とプロトコルがサポートするセキュリティ機能だけが **セキュリティプロファイル設定** ウィンドウに表示されます。

前提条件

電話セキュリティ プロファイルを設定する前に、次の情報を考慮してください。

- 電話を設定する際、**[電話の設定]** ウィンドウでセキュリティプロファイルを選択してください。デバイスがセキュリティまたはセキュアなプロファイルをサポートしていない場合、非セキュアなプロファイルを適用してください。
- 定義済みの安全ではないプロファイルを削除または変更することはできません。
- 現在デバイスに割り当てられているセキュリティプロファイルを削除することはできません。
- すでに電話に割り当てられているセキュリティプロファイルの設定を変更すると、再構成された設定が、その特定のプロファイルが割り当てられているすべての電話に適用されます。
- デバイスに割り当てられているセキュリティファイルの名前を変更することができます。以前のプロファイル名と設定で割り当てられた電話は、新しいプロファイル名と設定を引き継ぎます。
- CAPF 設定、認証モード、鍵サイズは **電話機の設定** ウィンドウに表示されます。 MIC または LSC を含む証明書操作のために CAPF 設定を構成する必要があります。 これらのフィールドは [**電話機の設定**] ウィンドウで直接更新できます。
- セキュリティプロファイルで CAPF 設定を更新すると、[**電話機の設定**] ウィンドウの設定も更新されます。
- [電話機の設定] ウィンドウの CAPF 設定を更新し、一致するプロファイルが見つかった場合、 Unified Communications Manager は一致するプロファイルを電話に適用します。
- [電話の設定] ウィンドウで CAPF 設定を更新し、一致するプロファイルが見つからない場合、システム Unified Communications Manager は新しいプロファイルを作成し、そのプロファイルを電話に適用します。
- アップグレード前にデバイスのセキュリティモードを構成している場合、システム Unified Communications Manager はそのモデルとプロトコルに基づいたプロファイルを作成し、デバイスに適用します。
- LSC のインストールのみに MIC を使用することをお勧めします。 Cisco は Unified Communications Manager での TLS 接続を認証するために LSC をサポートしています。 MIC ルート証明書は危険にさらされる可能性があるため、TLS 認証のために、またはその他の目的で MIC を使用するように電話を設定するユーザは、自身の責任でそうします。 MIC が侵害された場合、Cisco はその責任を負いません。

- 互換性の問題を避けるために、TLS 接続に LSC を使用するように Cisco IP 電話をアップグレードし、CallManager 信頼ストアから MIC ルート証明書を削除することを推奨します。

電話セキュリティ プロファイルの設定項目

次の表に、SCCP を実行する電話機のセキュリティ プロファイルの設定項目の説明を示します。

選択した電話機タイプおよびプロトコルがサポートしている設定だけが表示されます。

表 *26 : SCCP* を実行している電話のセキュリティ プロファイル

設定	説明
名前	セキュリティ プロファイルの名前を入力します。 新しいプロファイルを保存すると、電話タイプとプロトコルの **[電話の設定(Phone Configuration)]** ウィンドウの **[デバイスセキュリティ プロファイル(Device Security Profile)]** ドロップダウン リストにその名前が表示されます。 **ヒント** プロファイルの検索中またはプロファイルの更新中に正しいプロファイルを見つけるには、デバイスモデルとプロトコルをセキュリティ プロファイル名に含めます。
説明	セキュリティ プロファイルの説明を入力します。 説明には、どの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

設定	説明
[デバイスセキュリティモード(Device Security Mode)]	

設定	説明
	ドロップダウン リストから、次のオプションのいずれかを選択します。 • **[非セキュア(Non Secure)]**：電話機では、イメージ認証、ファイル認証、またはデバイス認証以外のセキュリティ機能を使用できません。 TCP 接続で Unified Communications Manager が利用できます。 • **認証のみ(Authenticated)**： Unified Communications Managerは電話機の整合性と認証を提供します。 NULL/SHA を使用する TLS 接続がシグナリングに対して開きます。 • **暗号化（Encrypted）**: Unified Communications Managerはトランクの整合性、シグナリング、および認証を提供します。 説明したように、次の暗号方式がサポートされています。 **TLS暗号方式** このパラメータは、Unified Communications Manager で SIP TLS 接続およびインバウンドの CTI Manager TLS CTI 接続を確立するためにサポートされる暗号を定義します。 最も強力：AES-256 SHA-384 のみ：RSA 優先 • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` （注） パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。 このオプションを選択すると、電話機は認証モードで登録されません。 最も強力：AES-256 SHA-384 のみ：ECDSA 優先 • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES256_GCM_SHA384` 中程度：AES-256 AES-128 のみ：RSA 優先 （注） パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。 このオプションを選択すると、電話機は認証モードで登録されません。 • `TLS_ECDHE_RSA with AES256_GCM_SHA384` • `TLS_ECDHE_ECDSA with AES256_GCM_SHA384` • `TLS_ECDHE_RSA with AES128_GCM_SHA256`

設定	説明
	• TLS_ECDHE_ECDSA with AES128_GCM_SHA256 （注） このオプションを選択した場合、パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。 このオプションを選択すると、電話機は認証モードで登録されません。 中程度：AES-256 AES-128 のみ：ECDSA 優先 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256 （注） このオプションを選択した場合、パラメータ [SRTP暗号方式（SRTP Ciphers）] の値を [最も強力 - AEAD AES-256 GCM 暗号のみ（Strongest - AEAD AES-256 GCM cipher only）] に設定することを強くお勧めします。 このオプションを選択すると、電話機は認証モードで登録されません。 すべての暗号方式: RSA優先 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES128_GCM_SHA256 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_RSA with AES_128_CBC_SHA1 すべての暗号 ECDSA 優先 • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 • TLS_ECDHE_RSA with AES128_GCM_SHA256

設定	説明
	• TLS_RSA with AES_128_CBC_SHA1 （注） 認証済みとして選択されている [デバイスのセキュリティ プロファイル (トランク)] を使用して設定した場合、 Unified Communications Manager は、NULL_SHA 暗号を使用した TLS connection (データ暗号化なし) を開始します。 これらのトランクは、通知先デバイスが NULL_SHA 暗号をサポートしていない場合は、そのデバイスを登録したり、コールを発信したりしません。 NULL_SHA 暗号をサポートしていない通知先デバイスでは、[暗号化 (Encrypted)] として選択した [デバイスのセキュリティ プロファイル (トランク)] で設定する必要があります。 このデバイス セキュリティ プロファイルを使用すると、トランクは、データの暗号化を可能にする追加の TLS 暗号を提供します。
[TFTP暗号化設定 (TFTP Encrypted Config)]	このチェックボックスがオンの場合、Unified Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイルを暗号化します。

設定	説明
認証モード（Authentication Mode）	

設定	説明
	このフィールドでは、CAPF 証明書の処理中に電話機が使用する認証方法を選択できます。 ドロップダウン リスト ボックスから、次のオプションのいずれかを選択します。 • **By Authentication String**—ユーザが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストールまたはアップグレード、削除またはトラブルシューティングします。 • **By Null String**—ユーザの介入なしで、ローカルで有効な証明書をインストールまたはアップグレード、削除またはトラブルシューティングします。 このオプションはセキュリティを提供しません。 このオプションは、閉鎖された安全な環境だけで選択することをお勧めします。 • **既存の証明書（LSC優先)**—製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話機に存在する場合、LSCをインストール、アップグレード、削除、またはトラブルシューティングします。 電話機にLSCが存在する場合、MICが電話機に存在するかどうかに関係なく、認証はLSCを介して行われます。 MICとLSCが電話機に存在する場合、認証はLSCを介して行われます。 電話機にLSCが存在せず、MICが存在する場合、認証はMICを通じて行われます。 このオプションを選択する前に、電話機内に証明書が存在することを確認してください。 このオプションを選択し、電話機内に証明書が存在しない場合、処理は失敗します。 MICとLSCは電話機に同時に存在できますが、電話機はCAPFに対する認証に1つの証明書のみを使用します。 優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • **既存証明書（MIC 優先）**—電話に LSC または MIC が存在する場合に、製造元でインストールされる証明書をインストールまたはアップグレード、削除またはトラブルシューティングします。 MICが電話機に存在する場合、LSCが電話機に存在するかどうかに関係なく、認証はMICを介して行われます。 電話機にLSCが存在し、MICが存在しない場合、認証はLSCを介して行われます。 このオプションを選択する前に、電話機内に証明書が存在することを確認してください。 このオプションを選択し、電話機内に証明書が存在しない場合、処理は失敗します。 （注）

設定	説明
	[電話セキュリティプロファイル(Phone Security Profile)]ウィンドウで設定される CAPF 設定値は、[電話の設定(Phone Configuration)]ウィンドウで設定される CAPF パラメータと相互に関係があります。
キー順序（Key Order）	このフィールドは、CAPF のキーの並び方を指定します。 ドロップダウン リストから、次のいずれかの値を選択します： • **RSA のみ** • **EC のみ** • **EC 優先、RSA バックアップ** （注） **キー順序（Key Order）**、**RSA キーサイズ（RSA Key Size）**、および **EC キーサイズ（EC Key Size）** フィールドの値に基づいて電話を追加すると、デバイスセキュリティプロファイルがその電話に関連付けられます。 256 ビットの **[EC キー サイズ（EC Key Size）]** 値で **[ECのみ（EC Only）]** 値を選択した場合は、デバイス セキュリティ プロファイルに **EC-256** 値が追加されます。
RSA キー サイズ（ビット）（RSA Key Size (Bits)）	ドロップダウンリストボックスから、次のいずれかの値を選択します。**512**、**1024**、**2048**、**3072**、または **4096**。 （注） CallManager **証明書の目的**で選択された RSA **キーの長さ**が 2048 を超えると、電話機の機種によっては登録に失敗することがあります。 *Cisco Unified Reporting Tool*（*CURT*）の *Unified CM* 電話機能リストレポートから、3072/4096 RSA キーサイズサポート機能でサポートされている電話モデルのリストを確認できます。
EC キーサイズ（ビット）	ドロップダウンリストから、**256**、**384**、または**521**のいずれかの値を選択します。

次の表に、SIP を実行する電話機のセキュリティ プロファイルの設定項目の説明を示します。

表 *27 : SIP* を実行している電話機のセキュリティ プロファイル

設定	説明
名前	セキュリティ プロファイルの名前を入力します。 新しいプロファイルを保存すると、電話タイプとプロトコルの **[電話の設定(Phone Configuration)]** ウィンドウの **[デバイスセキュリティプロファイル(Device Security Profile)]** ドロップダウン リストにその名前が表示されます。 **ヒント** セキュリティ プロファイル名にデバイス モデルとプロトコルを含めると、プロファイルを検索または更新する場合の適切なプロファイルの検出に役立ちます。
説明	セキュリティ プロファイルの説明を入力します。
[ナンス確認時間(Nonce Validity Time)]	ナンス値が有効な時間を秒単位で入力します。 デフォルト値は 600（10 分）です。 この時間が経過すると、Unified Communications Manager は新しい値を生成します。 （注） ナンス値は、ダイジェスト認証をサポートするランダム値で、ダイジェスト認証パスワードの MD5 ハッシュの計算に使用されます。

設定	説明
[デバイスセキュリティモード(Device Security Mode)]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • **[非セキュア(Non Secure)]**：電話機では、イメージ認証、ファイル認証、またはデバイス認証以外のセキュリティ機能を使用できません。 TCP 接続で Unified Communications Manager が利用できます。 • **認証のみ(Authenticated)**： Unified Communications Managerは電話機の整合性と認証を提供します。 NULL/SHA を使用する TLS 接続がシグナリングに対して開きます。 • **Encrypted**： Unified Communications Managerは電話機の整合性、認証、および暗号化を提供します。シグナリング用にAES128/SHAを使用するTLS接続を開始し、すべてのSRTP対応ホップ上のすべての電話機コールのメディアを SRTP で搬送します。 （注） 認証済みとして選択されている [デバイスのセキュリティ プロファイル (トランク)] を使用して設定した場合、 Unified Communications Manager は、NULL_SHA 暗号を使用した TLS connection (データ暗号化なし) を開始します。 これらのトランクは、通知先デバイスがNULL_SHA暗号をサポートしていない場合は、そのデバイスを登録したり、コールを発信したりしません。 NULL_SHA 暗号をサポートしていない通知先デバイスでは、[暗号化 (Encrypted)] として選択した [デバイスのセキュリティ プロファイル (トランク)] で設定する必要があります。 このデバイス セキュリティ プロファイルを使用すると、トランクは、データの暗号化を可能にする追加のTLS暗号を提供します。

設定	説明
[転送タイプ(Transport Type)]	[Device Security Mode] が **Non Secure** の場合は、ドロップダウン リストから次のオプションのいずれかを選択します（一部のオプションは表示されないことがあります）。 • **[TCP]**：パケットを送信された順に受信するには、Transmission Control Protocol を選択します。 このプロトコルは、パケットがドロップされないことを保証しますが、セキュリティは提供されません。 • **[UDP]**：パケットを高速に受信するには、User Datagram Protocol を選択します。 このプロトコルは、パケットをドロップすることがあり、送信された順に受信するとは限りません。 セキュリティは提供されません。 • **[TCP + UDP]**：TCP と UDP を組み合わせて使用するには、このオプションを選択します。 このオプションでは、セキュリティは提供されません。 [デバイスセキュリティモード(Device Security Mode)] が **[認証のみ(Authenticated)]** または **[暗号化(Encrypted)]** である場合、[TLS] が転送タイプとなります。 TLS では、SIP 電話のシグナリング整合性、デバイス認証、およびシグナリング暗号化（暗号化モードのみ）が提供されます。 プロファイルでデバイス セキュリティ モードを設定できない場合、転送タイプは UDP になります。
[ダイジェスト認証を有効化(Enable Digest Authentication)]	このチェックボックスをオンにすると、Unified Communications Manager は、電話機からのすべての SIP 要求でチャレンジを行います。 ダイジェスト認証ではデバイス認証、整合性、機密性は提供されません。 これらの機能を使用するには、セキュリティ モード [認証のみ(Authenticated)] または [暗号化(Encrypted)] を選択します。
[TFTP暗号化設定(TFTP Encrypted Config)]	このチェックボックスがオンの場合、Unified Communications Manager は電話機が TFTP サーバからダウンロードする設定ファイルを暗号化します。 このオプションは、Cisco 製電話機専用です。 **ヒント** このオプションを有効にして、対称キーを設定し、ダイジェスト信用証明書と管理者パスワードを保護することをお勧めします。

設定	説明
[OAuth 認証の有効化（Enable OAuth Authentication）]	このチェックボックスは、**デバイスセキュリティプロファイル**ドロップダウンリストから**暗号化**を選択した場合に使用できます。 このチェックボックスをオンにすると、Unified Communications Managerでは、電話セキュリティプロファイルに関連付けられているデバイスをSIP OAuthポートに登録することができるようになるます。 デフォルトでは、このチェックボックスはオフになっています。 次の場合に SIP OAuth を有効にすることができます： • [Transport Type] が [TLS] の場合。 • 端末セキュリティモードが暗号化されている場合。 • ダイジェスト認証が無効の場合。 • 暗号化設定が無効の場合。 （注） Unified Communications Manager リリース12.5以降、Jabberデバイスは SIP OAuth認証に対応しています。
[設定ファイル内のダイジェスト信用証明書を除外（Exclude Digest Credentials in Configuration File）]	このチェックボックスがオンの場合、 Unified Communications Managerは電話機が TFTP サーバからダウンロードする設定ファイル内のダイジェスト信用証明書を削除します。 このオプションは、Cisco IP Phone、7942、および7962（SIPのみ）に存在します。

設定	説明
認証モード（Authentication Mode）	

設定	説明
	このフィールドでは、CAPF 証明書の処理中に電話機が使用する認証方法を選択できます。 このオプションは、Cisco 製電話機専用です。 ドロップダウン リストから、次のオプションのいずれかを選択します。 • **By Authentication String**—ユーザが電話に CAPF 認証文字列を入力した場合にのみ、ローカルで有効な証明書をインストールまたはアップグレード、またはトラブルシューティングします。 • **By Null String**—ユーザの介入なしで、ローカルで有効な証明書をインストールまたはアップグレード、またはトラブルシューティングします。 このオプションではセキュリティが確保されません。したがって、セキュアな閉じた環境の場合にだけこのオプションを選択することをお勧めします。 • **既存の証明書（LSC優先)**—製造元でインストールされる証明書（MIC）またはローカルで有効な証明書（LSC）が電話機に存在する場合、LSCをインストール、アップグレード、またはトラブルシューティングします。 電話機にLSCが存在する場合、MICが電話機に存在するかどうかに関係なく、認証はLSCを介して行われます。 電話機にLSCが存在せず、MICが存在する場合、認証はMICを介して行われます。 このオプションを選択する前に、電話機内に証明書が存在することを確認してください。 このオプションを選択し、電話機内に証明書が存在しない場合、処理は失敗します。 MICとLSCは電話機に同時に存在できますが、電話機はCAPFに対する認証に1つの証明書のみを使用します。 優先されるプライマリ証明書が何らかの理由で破損した場合、または別の証明書を使用して認証を受ける場合は、認証モードを更新する必要があります。 • **既存証明書（MIC 優先）**—電話に LSC または MIC が存在する場合に、製造元でインストールされる証明書をインストールまたはアップグレードまたはトラブルシューティングします。 MICが電話機に存在する場合、LSCが電話機に存在するかどうかに関係なく、認証はMICを介して行われます。 電話機にLSCが存在し、MICが存在しない場合、認証はLSCを介して行われます。 このオプションを選択する前に、電話機内に証明書が存在することを確認してください。 このオプションを選択し、電話機内に証明書が存在しない場合、処理は失敗します。 （注） [電話セキュリティプロファイル(Phone Security Profile)]ウィンドウで

設定	説明
	設定される CAPF 設定値は、[電話の設定(Phone Configuration)]ウィンドウで設定される CAPF パラメータと相互に関係があります。
[キーサイズ(Key Size)]	CAPF で使用されるこの設定では、ドロップダウンリストから証明書のキー サイズを選択します。 デフォルト設定は 1024 です。キーサイズに 512 を選ぶこともできます。 デフォルトの設定よりも大きいキー サイズを選択した場合、キーの生成に必要なエントロピーを生成するために長い時間がかかります。キー生成の優先順位を低く設定すると、処理中に電話機を動作させることができます。 電話機のモデルによっては、キー生成が完了するまでに 30 分以上かかることがあります。 （注） [電話セキュリティプロファイル(Phone Security Profile)]ウィンドウで設定される CAPF 設定値は、[電話の設定(Phone Configuration)]ウィンドウで設定される CAPF パラメータと相互に関係があります。
[SIP電話ポート(SIP Phone Port)]	この設定は、UDP 転送を使用し SIP を実行する電話に適用されます。 UDP を使用する Cisco Unified IP 電話（SIP のみ）が、Unified Communications Manager からの SIP メッセージの傍受に使用するポート番号を入力します。 デフォルト設定は 5060 です。 TCP または TLS を使用する電話機は、この設定を無視します。

電話セキュリティ設定のタスクフロー

次のタスクを実行して、電話セキュリティを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	（任意） 電話セキュリティ プロファイルの検索 （160 ページ）	電話セキュリティ プロファイルを検索して電話を保護します。
ステップ 2	電話セキュリティ プロファイルのセットアップ	電話セキュリティ プロファイルをセットアップして電話を保護します。
ステップ 3	電話セキュリティ プロファイルを適用する	電話セキュリティ プロファイルを適用して電話を保護します。
ステップ 4	電話セキュリティ プロファイルと電話を同期する	すべての電話セキュリティプロファイルを選択した電話と同期します。

	コマンドまたはアクション	目的
ステップ 5	（任意） 電話セキュリティ プロファイルの削除	電話に関連付けられたすべての電話セキュリティプロファイルを削除します。
ステップ 6	電話セキュリティ プロファイルで電話を検索する	電話セキュリティ プロファイルに関連付けられたすべての電話を検索します。
ステップ 7	SIP トランク セキュリティ プロファイルの相互作用と制限	SIP トランク セキュリティ プロファイルの相互作用と制限

電話セキュリティ プロファイルの検索

電話セキュリティプロファイルを検索するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administration から **[システム（System）] > > [セキュリティプロファイル（Security Profile）] > > [電話セキュリティプロファイル（Phone Security Profile）]** を選択します。

このウィンドウには、アクティブな（以前の）クエリーのレコードも表示されることがあります。

ステップ 2 データベース内のすべてのレコードを検索するには、ダイアログボックスが空になっていることを確認し、ステップ 3 （160 ページ） に進みます。

レコードをフィルタまたは検索する手順は、次のとおりです。

a) 最初のドロップダウンリストから、検索パラメータを選択します。
b) 2 番目のドロップダウンリストから、検索パターンを選択します。
c) 必要に応じて、適切な検索テキストを指定します。

（注）
さらに検索条件を追加するには、[+] ボタンをクリックします。 条件を追加した場合は、指定したすべての条件に一致するレコードが検索されます。 条件を削除する場合、最後に追加した条件を削除するには、**[-]**ボタンをクリックします。追加した検索条件をすべて削除するには、**[フィルタのクリア（Clear Filter）]** ボタンをクリックします。

ステップ 3 **[検索（Find）]** をクリックします。

一致するすべてのレコードが表示されます。 [ページあたりの行数(Rows per Page)]ドロップダウン リストから異なる値を選択すると各ページに表示される項目数を変更できます。

ステップ 4 表示されたレコード リストから、目的のレコードのリンクをクリックします。

（注）

ソート順を逆にするには、リストのヘッダーにある上矢印または下矢印をクリックします（使用可能な場合）。

選択したレコードがウィンドウに表示されます。

電話セキュリティ プロファイルのセットアップ

電話セキュリティプロファイルをセットアップするには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administration から **[システム（Systems）] > [セキュリティプロファイル（Security Profile）] > [電話セキュリティプロファイル（Phone Security Profile）]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

a) 新しいプロファイルを追加するには、[**新規追加**] をクリックします。

b) 既存のセキュリティプロファイルをコピーするには、適切なプロファイルを見つけて、コピーするセキュリティプロファイルの隣にある [**コピー**] をクリックして続行します。

c) 既存のプロファイルを更新するには、適切なセキュリティプロファイルを見つけて続行します。

新規作成をクリックすると、設定ウィンドウの各フィールドが既定の設定で表示されます。 [**コピー**] をクリックすると、構成ウィンドウにコピーした設定が表示されます。

ステップ 3 SCCP または SIP を使用している電話に適切な設定を入力します。

ステップ 4 **[保存（Save）]** をクリックします。

電話へのセキュリティ プロファイルの適用

証明書を使用するセキュリティプロファイルを電話の認証に適用する前に、特定の電話にローカルで有効な証明書 (LSC) または製造元でインストールされた証明書 (MIC) が含まれていることを確認してください。

電話機のセキュリティ機能を使用可能にするには、デバイスタイプとプロトコルに対応した新しいセキュリティ プロファイルを設定して電話機に適用する必要があります。 ただし、電話に証明書が含まれていない場合は、次のタスクを実行してください。

- **[電話機の設定（Phone Configuration）]** ウィンドウで、非セキュアプロファイルを適用してください。
- **電話設定** ウィンドウで CAPF 設定を行い、証明書をインストールします。

- **[電話機の設定（Phone Configuration）]** ウィンドウで、認証または暗号化が設定されているデバイス セキュリティ プロファイルを適用します。

電話セキュリティ プロファイルをデバイスに適用するには、次の手順を実行します。

手順

ステップ 1 **[電話機の設定]** ウィンドウの **[プロトコル固有情報（Protocol Specific Information）]** セクションに移動します。

ステップ 2 [**端末セキュリティプロファイル**] ドロップダウンリストから、端末に適用するセキュリティ プロファイルを選択します。
電話タイプとプロトコルだけに設定されている電話セキュリティ プロファイルが表示されます。

ステップ 3 **[保存（Save）]** をクリックします。

ステップ 4 変更を適切な電話に適用するには、 **[設定の適用]** をクリックします。

（注）
セキュリティプロファイルを削除するには、**[検索と一覧表示（Find and List）]** ウィンドウで適切なセキュリティプロファイルの隣にあるチェックボックスを選択し、**[選択項目の削除（Delete Selected）]** をクリックします。

電話セキュリティ プロファイルを電話と同期する

電話セキュリティ プロファイルを電話と同期するには、次の手順を実行します。

手順

ステップ 1 Unified Communications Manager Administration で **[システム]** > **セキュリティプロファイル** > **[電話セキュリティプロファイル]**を選択します。

ステップ 2 使用する検索条件を選択し、[検索（Find）]をクリックします。
ウィンドウには、検索基準に一致する電話セキュリティ プロファイルのリストが表示されます。

ステップ 3 適用する電話を同期する電話セキュリティ プロファイルをクリックします。

ステップ 4 追加の設定変更を加えます。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 **[設定の適用（Apply Config）]** をクリックします。
[**設定情報の適用**] ダイアログボックスが表示されます。

ステップ 7 **OK**をクリックします。

電話セキュリティ プロファイルの削除

Unified Communications Managerからセキュリティプロファイルを削除する前に、デバイスに別のプロファイルを適用するか、そのプロファイルを使用するすべてのデバイスを削除する必要があります。

プロファイルを使用するデバイスを見つけるには、ステップ 1 を実行します。

手順

ステップ 1 **[セキュリティプロファイルの設定（Security Profile Configuration）]** ウィンドウで、**[関連リンク（Related Links）]** のドロップダウンメニューから **[依存関係レコード（Dependency Records）]** を選択し、**[移動（Go）]** をクリックします。

システムで依存関係レコード機能が有効になっていない場合は、**[システム（System）]**>**[エンタープライズパラメータ設定（Enterprise Parameters Configuration）]** に移動して、[依存関係レコードを有効にする（Enable Dependency Records）] 設定を **[はい（True）]** に変更します。依存関係レコード機能に関連する、高い CPU 使用率に関する情報がメッセージに表示されます。 変更を保存して依存関係レコードをアクティブにします。 依存関係レコードの詳細については、次を参照してください。 Cisco Unified Communications Manager システム設定ガイド

このセクションでは、Unified Communications Managerデータベースから電話セキュリティプロファイルを削除する方法について説明します。

ステップ 2 削除するセキュリティプロファイルを見つけてください。

ステップ 3 セキュリティプロファイルを削除するには、**[検索と一覧表示（Find and List）]** ウィンドウで適切なセキュリティプロファイルの隣にあるチェックボックスを選択し、**[選択項目の削除（Delete Selected）]** をクリックします。 **[すべて選択(Select All)]** をクリックして **[選択項目の削除(Delete Selected)]** をクリックすると、この選択対象として設定可能なすべてのレコードを削除できます。

ステップ 4 単一のセキュリティプロファイルを削除するには、以下のいずれかのタスクを実行します。

a) [**検索と一覧表示**] ウィンドウで適切なセキュリティプロファイルのチェックボックスを選択します。それから **選択項目を削除**をクリックします。

ステップ 5 削除の確認が求められたら、[**OK**] をクリックして削除するか、または [**キャンセル**] をクリックして削除操作をキャンセルします。

電話セキュリティ プロファイルで電話を検索する

特定のセキュリティ プロファイルを使用する電話を検索するには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administration から、**[デバイス（Device）] > > [電話機（Phone）]** を選択します。

ステップ 2 最初のドロップダウンリストから、検索パラメータ **セキュリティプロファイルを選択します**。

a) ドロップダウン リストから、検索パターンを選択します。

b) 必要に応じて、適切な検索テキストを指定します。

（注）
さらに検索条件を追加するには、**[+]** をクリックします。 条件を追加した場合は、指定したすべての条件に一致するレコードが検索されます。 条件を削除する場合、最後に追加した条件を削除するには、**[-]** ボタンをクリックします。追加した検索条件をすべて削除するには、**[フィルタのクリア（Clear Filter）]** ボタンをクリックします。

ステップ 3 **[検索（Find）]** をクリックします。

一致するすべてのレコードが表示されます。 1 ページあたりの項目の表示件数を変更するには、[ページあたりの行数（Rows per Page）] ドロップダウンリストで別の値を選択します。

ステップ 4 表示されたレコード リストから、目的のレコードのリンクをクリックします。

（注）
ソート順を逆にするには、リストのヘッダーにある上矢印または下矢印をクリックします（使用可能な場合）。

選択したレコードがウィンドウに表示されます。

SIP トランク セキュリティ プロファイルの相互作用と制限

次の表には、SIP トランクセキュリティプロファイルの機能の相互作用と制限が含まれています。

表 *28 : SIP* トランク セキュリティ プロファイルの相互作用と制限

機能	連携動作と制限事項
90 日間の評価ライセンス	90 日の評価期間を使用して実行している間、セキュア SIP トランクを導入することはできません。セキュア SIP トランクを導入するには、製品登録トークンで **[輸出規制による機能限定の許可（Allow export-controlled functionality）]** を選択した Smart Software Manager アカウントにシステムを登録してある必要があります。

SIP 電話のダイジェスト認証の概要

ダイジェスト認証により、Unified Communications Manager は SIP を実行している電話に対する要求メッセージをチャレンジできます。 これには、キープアライブを除くすべての要求メッセージが含まれます。 Unified Communications Managerは、 **エンドユーザー設定** ウィンドウで設定された通り、電話が提供する資格情報を検証するために、エンドユーザーをダイジェスト資格情報を通じて認証します。

電話がエクステンション モビリティをサポートしている場合、エクステンション モビリティのユーザがログインするときに、Unified Communications Managerは **エンドユーザー設定** ウィンドウで設定されたエクステンションモビリティのエンドユーザーのダイジェスト資格情報を使用します。

SIP 電話のダイジェスト認証の前提条件

デバイスのダイジェスト認証を有効にすると、デバイスを登録するための一意のダイジェストユーザ ID とパスワードが要求されます。 電話ユーザまたはアプリケーションユーザに対して、Unified Communications Manager データベースで SIP ダイジェスト資格情報を設定する必要があります。

次のことを確認してください:

- アプリケーションの場合は、[アプリケーションユーザーの設定（Application User Configuration）] ウィンドウでダイジェスト認証情報を指定します。
- SIP を実行している電話の場合、[エンドユーザの構成] ウィンドウでダイジェスト認証の資格情報を指定します。

  ユーザを設定した後で電話に資格情報を関連付けるには、[電話の設定] ウィンドウで [ダイジェスト ユーザ] を選択します。 電話をリセットすると、TFTP サーバが電話に提供する電話設定ファイルに資格情報が含まれるようになります。
- SIP トランクで受信したチャレンジについては、領域ユーザ名 (デバイスまたはアプリケーション ユーザ) とダイジェスト資格情報を指定する SIP 領域を設定します。

（注） クラスタ セキュリティ モードはダイジェスト認証には影響しないことに注意してください。

SIP 電話のダイジェスト認証の設定タスク フロー

これらのタスクを完了して SIP 電話のダイジェスト認証を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	電話ユーザーにダイジェスト信用証明書を指定する	ダイジェスト クレデンシャルを、電話を所有するエンドユーザに割り当てます。
ステップ 2	電話セキュリティ プロファイルでダイジェスト認証を有効にする	電話に関連付けられている電話セキュリティ プロファイルでダイジェスト認証を有効にします。
ステップ 3	電話にダイジェスト認証を指定する	[電話の設定] で、ユーザをダイジェスト ユーザとして割り当てます。 ダイジェスト認証が有効なセキュリティプロファイルが割り当てられていることを確認してください。
ステップ 4	エンドユーザーのダイジェスト認証情報の設定	エンドユーザのダイジェスト認証情報を設定します。
ステップ 5	SIP ステーションレルムの設定（167 ページ）	Unified CM が 401 未承認メッセージによる SIP リクエストにチャレンジするために使用する、[領域] フィールドの文字列を指定します。

電話ユーザーにダイジェスト信用証明書を指定する

この手順を使用して、電話を所有するエンドユーザにダイジェスト認証情報を割り当てます。電話は資格情報を使用して認証します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから **ユーザ管理** > **エンドユーザ**を選択します。

ステップ 2 **検索** をクリックし、電話を所有するユーザを選択します。

ステップ 3 以下のフィールドに資格情報を入力します。

- [ダイジェスト信用証明書(Digest Credentials)]
- [ダイジェスト信用証明書の確認(Confirm Digest Credentials)]

ステップ 4 **[保存（Save）]** をクリックします。

電話セキュリティ プロファイルでダイジェスト認証を有効にする

電話セキュリティプロファイルを通じて電話のダイジェスト認証を有効にするには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[セキュリティ（Security）]** > **[電話セキュリティプロファイル（Phone Security Profile）]** の順に選択します。

ステップ 2 **検索** をクリックして、その電話に関連付けられている電話セキュリティプロファイルを選択します。

ステップ 3 [ダイジェスト認証を有効化（Enable Digest Authentication）]チェックボックスをオンにします。

ステップ 4 **[保存（Save）]** をクリックします。

電話にダイジェスト認証を指定する

この手順を使用してダイジェストユーザとダイジェスト認証有効化セキュリティプロファイルを電話に関連付けます。

手順

ステップ 1 Cisco Unified Communications Manager Administration から、**[デバイス（Device）]** > **[電話機（Phone）]** を選択します。

ステップ 2 [**検索**] をクリックして、ダイジェスト認証を指定する電話を選択します。

ステップ 3 **[ダイジェストユーザー（Digest User）** ドロップダウンメニューから、ダイジェスト認証を割り当てたエンドユーザーを指定します。

ステップ 4 ダイジェスト認証を有効にした電話セキュリティプロファイルが、[**デバイスセキュリティプロファイル**] ドロップダウンリストから割り当てられていることを確認してください。

ステップ 5 **[保存（Save）]** をクリックします。

ステップ 6 [**リセット（Reset）**] をクリックします。

エンドユーザを電話に関連付けた後、設定を保存し、電話をリセットします。

SIP ステーションレルムの設定

401 Unauthorized メッセージへの応答で SIP 電話にチャレンジするときに、Cisco Unified Communications Manager が [領域] フィールドで使用する文字列を指定します。 これは、電話がダイジェスト認証に設定されている場合に適用されます。

（注） このサービスパラメータのデフォルトの文字列は ccmsipline です。

手順

ステップ 1 Unified Communications Manager で、**[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

ステップ 2 **[サーバ]** ドロップダウンリストから、CiscoCallManager サービスを有効にしたノードを選択します。

ステップ 3 **サービス** ドロップダウンリストから CiscoCallManager サービスを選択します。 サービス名の横に「「アクティブ」」と表示されていることを確認します。

ステップ 4 ヘルプに記載されているとおり、 **SIP レルムステーション** パラメータを更新してください。 パラメータのヘルプを表示するには、疑問符またはパラメータ名のリンクをクリックします。

ステップ 5 **[保存（Save）]** をクリックします。

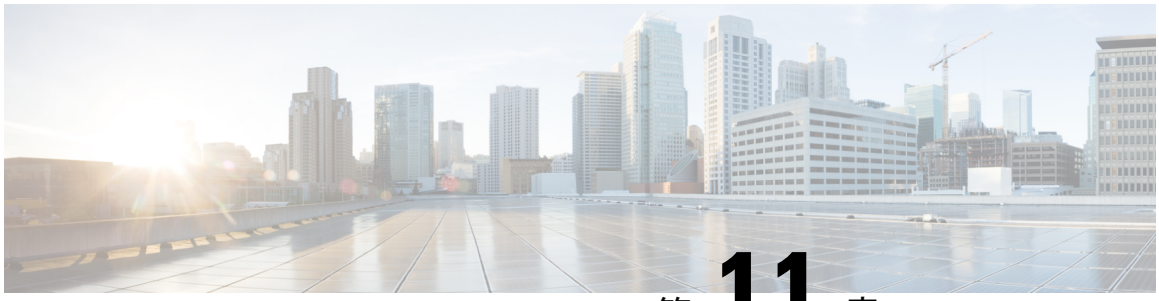
エンドユーザーのダイジェスト認証情報の設定

ダイジェスト認証情報の詳細を表示するには、以下の手順を実行します。

Cisco Unified Communications Manager Administration で、**[ユーザー管理（User Management ）]** > **[エンドユーザー（End User）]** にアクセスし、ユーザー ID をクリックすると、**[エンドユーザーの設定（End User Configuration）]** ウィンドウが表示されます。 ダイジェスト認証情報は、**[エンドユーザーの設定（End User Configuration）]** ウィンドウの **[ユーザー情報（User Information）]** ペインから入手できます。

表 *29 : [ダイジェスト信用証明書(Digest Credentials)]*

設定	説明
[ダイジェスト信用証明書(Digest Credentials)]	英数字文字列を入力します。
[ダイジェスト信用証明書の確認(Confirm Digest Credentials)]	ダイジェスト信用証明書を正しく入力したことを確認するために、このフィールドにクレデンシャルを入力します。



第 11 章

セキュアな電話会議リソースのセットアップ

この章では、安全な電話会議リソースの設定について説明します。

- セキュアな会議 （169 ページ）
- 会議ブリッジの要件 （170 ページ）
- セキュア電話会議アイコン （171 ページ）
- セキュア電話会議の状況 （172 ページ）
- Cisco Unified IP Phone のセキュアな電話会議とアイコンのサポート （175 ページ）
- セキュアな会議 CTI サポート （176 ページ）
- トランクおよびゲートウェイでのセキュアな電話会議 （176 ページ）
- CDR データ （176 ページ）
- 連携動作と制限事項 （176 ページ）
- 電話会議リソースを保護するためのヒント （178 ページ）
- セキュアな電話会議ブリッジのセットアップ （180 ページ）
- Cisco Unified Communications Manager Administration でセキュアな電話会議ブリッジをセットアップする （181 ページ）
- ミートミー電話会議の最低セキュリティレベルのセットアップ （182 ページ）
- セキュアな電話会議用のパケットキャプチャのセットアップ （182 ページ）

セキュアな会議

セキュアな会議機能は、会議をセキュアにするための認証と暗号化を提供します。すべての参加デバイスでシグナリングとメディアが暗号化されている場合、会議は安全であると見なされます。 セキュアな電話会議機能は、セキュアな TLS または IPSec 接続での SRTP 暗号化をサポートします。

システムは、参加しているデバイスの最も低いセキュリティレベルによって決定される、会議の全体的なセキュリティステータスに対してセキュリティアイコンを提供します。 たとえば、2 つの暗号化された接続と 1 つの認証された接続を含む安全な会議の会議セキュリティ ステータスは認証済みです。

安全なアドホックおよびミートミー会議を設定するには、安全な会議ブリッジを設定します。

- ユーザが認証または暗号化された電話から会議通話を開始すると、 Unified Communications Manager がセキュアな会議ブリッジを割り当てます。
- ユーザが非セキュア電話から発信すると、 Unified Communications Manager は非セキュア電話会議ブリッジを割り当てます。

会議ブリッジ リソースをノンセキュアとして設定すると、電話のセキュリティ設定に関係なく、電話会議はノンセキュアのままになります。

（注） Unified Communications Manager は、電話会議を開始する電話の Media Resource Group List (MRGL) から会議ブリッジを割り当てます。 安全な会議ブリッジが利用できない場合、 Unified Communications Manager はノンセキュアな会議ブリッジを割り当て、会議はノンセキュアです。 安全な会議ブリッジが利用できない場合、 Unified Communications Manager はノンセキュアな会議ブリッジを割り当て、会議はノンセキュアです。 利用できる会議ブリッジがない場合、会議は失敗します。

ミートミーコンファレンスコールの場合、電話会議を開始する電話は、ミートミー番号に設定されている最小のセキュリティ要件も満たす必要があります。 セキュアなコンファレンスブリッジを利用できない場合、または開始者のセキュリティレベルが最低要件を満たさない場合、 Unified Communications Manager は電話会議を拒否します。

割り込みで電話会議をセキュアにするには、暗号化モードを使用するように電話を設定します。 割り込みキーが押され、デバイスが認証または暗号化された後、 Unified Communications Manager が割り込み側とターゲットデバイスの内蔵ブリッジの間の安全な接続を確立します。 システムは、バージコールに接続しているすべての側に対して、電話会議のセキュリティ ステータスを提供します。

（注） リリース 8.3 以降を実行している非セキュアまたは認証済み Cisco Unified IP Phone は、暗号化されたコールを割り込みできます。

会議ブリッジの要件

ハードウェアの Conference ブリッジをネットワークに追加し、Unified Communications Manager Administration でセキュアな会議ブリッジを設定するときに、会議ブリッジをセキュアなメディア リソースとして登録できます。

（注） Unified Communications Manager の処理に対するパフォーマンスの影響により、Cisco はソフトウェア会議ブリッジでのセキュアな電話会議をサポートしていません。

H.323 またはMGCP ゲートウェイ上で電話会議を提供するデジタル シグナル プロセッサ (DSP) ファームは、IP 電話会議のネットワーク リソースとして機能します。 コンファレンスブリッジは、セキュアなSCCP クライアントとしてUnified Communications Managerに登録されます。

- コンファレンスブリッジのルート証明書は、CallManagerの信頼ストアに存在している必要があり、Cisco CallManager証明書は、コンファレンスブリッジの信頼ストアに存在している必要があります。
- セキュアな電話会議ブリッジのセキュリティ設定が、登録する Unified Communications Manager のセキュリティ設定と一致している必要があります。

電話会議ルーターの詳細については、ルーターに付属のIOSルーターのマニュアルを参照してください。

Unified Communications Manager は、動的に電話会議リソースを通話に割り当てます。 利用可能な電話会議リソースと有効なコーデックにより、ルーターごとに同時に開催できるセキュアな電話会議の最大数が決まります。 送信および受信のストリームは、参加しているエンドポイントごとに個別にキーイングされるため (参加者が電話会議を退席したときに、キーの再生成は必要ありません)、DSPモジュールのセキュアな電話会議の総容量は、設定できるノンセキュアな容量の 2 分の 1 になります。

詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』 を参照してください。

セキュア電話会議アイコン

Cisco IP Phone には、電話会議全体のセキュリティレベルに応じた電話会議セキュリティアイコンが表示されます。 これらのアイコンは、お使いの電話機のユーザ ドキュメントに記載されている安全な 2 者間コールのステータス アイコンと対応しています。

通話の音声とビデオの部分が、電話会議のセキュリティレベルの基礎となります。 音声とビデオの両方が安全である場合に限り、通話は安全であると見なされます。

アドホックおよび Meet-Me セキュア会議では、電話会議のセキュリティ アイコンが、電話会議参加者に対して電話ウィンドウの電話会議ソフトキーの隣に表示されます。 表示されるアイコンは、電話会議ブリッジとすべての参加者のセキュリティレベルによって異なります。

- 会議ブリッジがセキュアで、電話会議のすべての参加者が暗号化されている場合は、ロックアイコンが表示されます。
- 会議ブリッジがセキュアで、電話会議のすべての参加者が認証されている場合は、盾アイコンが表示されます。 一部の電話モデルでは盾のアイコンが表示されません。
- 会議ブリッジまたは電話会議の参加者が非セキュアの場合、コール状態アイコン（アクティブ、保留など）が表示されます。一部の古い電話機モデルでは、アイコンは表示されません。

（注） パラメータ値が True で、音声が保護されている場合、「コールセキュリティステータスを指定するときにBFCPアプリケーション暗号化ステータスを上書きする（Override BFCP Application Encryption Status When Designating Call Security Status）] サービスパラメータはロックアイコンを表示します。 この条件は、他のすべてのメディア チャンネルのセキュリティ ステータスを無視します。 既定のパラメータ値は False です。

暗号化された電話がセキュアな会議ブリッジに接続すると、デバイスと会議ブリッジ間のメディアストリーミングが暗号化されます。ただし、会議のアイコンは、他の参加者のセキュリティレベルにより、暗号化される、認証される、または非セキュアになることがあります。非セキュアなステータスは、参加者の一部が安全ではない、または確認できないことを示します。

ユーザーが [バージ（Barge）] を押すと、[バージ（Barge）] ソフトキーの隣に表示されるアイコンが、会議のバージのセキュリティレベルを表示します。割り込みデバイスと割り込みデバイスが暗号化をサポートしている場合、システムは2つのデバイス間のメディアを暗号化しますが、割り込み会議のステータスは、接続者のセキュリティ レベルに応じて、非セキュア、認証済み、または暗号化になります。

セキュア電話会議の状況

参加者が電話会議に出入りするにつれて、電話会議の状況が変化します。認証された参加者または保護されていない参加者がコールに接続すると、暗号化された電話会議は認証されたまたは非セキュアなセキュリティレベルに戻ることができます。同様に、認証済みの参加者または安全ではない参加者が通話を切断した場合、状況は改善できます。セキュアではない参加者が電話会議に接続すると、電話会議が非セキュアになります。

電話会議の状況は、参加者が複数の電話会議を連鎖させるとき、連結された電話会議のセキュリティ状況が変更されるとき、保留中の電話会議が別のデバイスで再開されるとき、電話会議が割り込まれたとき、または転送された電話会議が別のデバイスに完了したときにも変更できます。

（注） Advanced Ad Hoc Conference Enabled サービスパラメータは、複数のアドホック会議を電話会議、参加、直接転送、転送などの機能を使用して相互にリンクできるかどうかを決定します。

Unified Communications Managerには、安全な電話会議を開催するためのオプションが用意されています。

- アドホック会議リスト
- 最低セキュリティ レベルの Meet-Me 電話会議

Ad Hoc 電話会議のリスト

電話会議中にConfListソフトキーを押すと、参加している電話機に電話会議リストが表示されます。各参加者の電話会議の状況およびセキュリティ状況を提供する電話会議リストは、暗号化されていない参加者を識別するために使用されます。

電話会議リストに表示されるセキュリティアイコンは、非セキュア、認証済み、暗号化、保留中です。 電話会議の開始者は電話会議リストを使用して、低セキュリティ ステータスの参加者を退出させることができます。

（注） Advanced Ad Hoc Conference Enabled サービスのパラメータにより、電話会議の開始者以外の参加者が会議参加者を退席させることができるかどうかが決定されます。

参加者が電話会議に参加すると、電話会議リストの一番上に追加されます。 ConfListおよびRmLstCソフトキーを使用して、セキュアな電話会議からセキュアではない参加者を削除するには、電話のユーザ ドキュメントを参照してください。

次のセクションでは、他の機能とのセキュアなアドホック会議の対話について説明します。

セキュアなアドホック会議と会議のチェーン

アドホック電話会議が別のアドホック電話会議に連結されている場合、連結された電話会議は、固有のセキュリティステータスを持つメンバー 「会議」 として表示されます。 Unified Communications Manager は、連結された会議のセキュリティレベルを含めて、電話会議全体のセキュリティ状況を判断します。

セキュアな Ad Hoc 電話会議と cBarge

ユーザーがアクティブな電話会議に参加するために cBarge ソフトキーを押すと、Unified Communications Manager がアドホック会議を作成し、割り込みのセキュリティレベルと MRGL に基づいて会議ブリッジを割り当てます。 cbarge メンバーの名前が電話会議リストに表示されます。

セキュアな Ad Hoc 電話会議と cBarge

セキュアなアドホック電話会議の参加者が割り込みを受けた場合、電話会議リストの割り込みターゲットの隣に、割り込みコールのセキュリティ ステータスが表示されます。割り込みターゲットのセキュリティアイコンは、実際には割り込みターゲットと電話会議ブリッジの間でメディアが暗号化されている場合でも、認証済みと表示される場合があります。これは、割り込み発信者には認証された接続があるためです。

割り込みのターゲットはセキュアですが、それがセキュアではないアドホック会議にある場合、アドホック会議の状況が後でセキュアに変更されると、割り込み発信者アイコンも更新されます。

セキュアな Ad Hoc 電話会議とジョイン

認証または暗号化された電話ユーザは、 Cisco Unified IP Phone (SCCP を実行している電話のみ) でJoin ソフトキーを使用して、セキュアなアドホック電話会議を作成したり、アドホック電話会議に参加したりできます。セキュリティステータスが未知の参加者を既存の電話会議に追加するためにユーザーが [参加（Join）] を押した場合、Unified Communications Manager は電話会議のステータスを不明に下げます。 [参加] で新しいメンバーを追加した参加者は電話会議の開始者になり、新しいメンバーや他の参加者を電話会議リストから外すことができます(Advanced Ad Hoc Conference Enabled 設定が True の場合)。

安全な Ad Hoc 電話会議および保留/再開

電話会議の開始者が、参加者を追加するために電話会議を保留にしても、電話会議のステータスは、追加された参加者が通話に応答するまで、不明 (非セキュア) のままになります。 新しい参加者が応答すると、電話会議リストの電話会議のステータスが更新されます。

共有回線上の発信者が別の電話で保留中の電話会議を再開した場合、発信者が [再開] を押すと、電話会議リストが更新されます。

最低セキュリティ レベルの Meet-Me 電話会議

管理者として、ミートミーコンファレンスのパターンまたは番号を非セキュア、認証、または暗号化として設定する場合、電話会議の最低セキュリティレベルを指定することができます。参加者はセキュリティの最低要件を満たさなければなりません。満たしていない場合、システムは参加者をブロックし、通話を切断します。このアクションは、ミートミーコンファレンスコールの転送、再開された共有回線上のミートミーコンファレンスコール、およびチェーンされたミートミーコンファレンスに適用されます。

ミートミーコンファレンスを開始する電話は、最低限のセキュリティレベルを満たす必要があります。満たさない場合、システムは試みを拒否します。最小セキュリティレベルが認証または暗号化を指定しており、セキュアな会議ブリッジが利用できない場合、通話は失敗します。

会議ブリッジングの最小レベルとして非セキュアを指定する場合、会議ブリッジングはすべての通話を受け入れ、会議のセキュリティステータスは非セキュアになります。

以下のセクションでは、他の機能との安全なミートミー電話会議の対話について説明します。

Meet-Me 電話会議および Ad Hoc 電話会議

ミートミー電話会議をアドホック会議に、またはアドホック会議をミートミー電話会議に追加するには、その Ad Hoc 電話会議がミートミー電話会議の最低セキュリティレベルを満たす必要があります。満たさない場合、通話は切断されます。 電話会議が追加されると、電話会議アイコンが変更されます。

Meet-Me 会議とバージ

発信者がミートミー電話会議の参加者にバージするときに、バージ発信者が最小セキュリティ要件を満たさない限り、バージデバイスのセキュリティレベルがダウングレードし、バージ発信者とバージコールの両方がドロップされます。

Meet-Me 電話会議およびホールド/リジューム

共有回線上の電話は、最低セキュリティレベルを満たさない限り、ミートミー電話会議を再開できません。 電話が最低セキュリティ レベルを満たしていない場合、ユーザが [再開] を押すと、共有回線上のすべての電話がブロックされます。

Cisco Unified IP Phone のセキュアな電話会議とアイコンのサポート

これらの Cisco Unified IP Phone はセキュアな会議とセキュアな会議のアイコンに対応しています:

- Cisco Unified IP Phones 7942 および 7962 (SCCP のみ、認証済みのセキュアな会議のみ)
- Cisco Unified IP Phone 6901、6911、6921、6941、6945、6961、7906G、7911G、 、79411、79411、7941, 7941G-GE, 7942G, 7945G, 7961G, 7961G-GE, 7962G, 7965G, 7975G, 8941, および 8945 (SCCP のみ)
- Cisco Unified IP Phone 6901, 6911, 6921, 6941, 6945, 6961, 7906G, 7911G, 7941G, 7941G-GE, 7942G, 7961G, 7961G-GE, 7962G, 7965G,

  Cisco IP 電話 7811、7821、7841、7861、 Cisco IP会議電話7832、 Cisco IP 電話 8811, 8841, 8845, 8851, 8851NR, 8861, 8865, 8865NR, Cisco ワイヤレスIP電話 8821, Cisco Unified IP会議電話 8831、 Cisco IP会議電話 8832。

警告 セキュアな電話会議機能を最大限に活用するには、 Cisco Unified IP Phone を 8.3 以降にアップグレードすることをおすすめします。このリリースの暗号化機能はサポートしています。 以前のリリースを実行する暗号化された電話はこれらの新機能を完全にサポートしません。 これらの電話はセキュアな電話会議に認証された参加者またはセキュアではない参加者としてのみ参加できます。

リリース 8.3 以前のリリースを使用している Unified Communications Manager で動作する Cisco Unified IP Phone は、接続のセキュリティステータスを表示し、会議のセキュリティステータスではない。会議リストのようなセキュアな会議機能はサポートしていません。

Unified Communications Manager のセキュアな会議の制限に関連するトピックを参照してください。これらの制限は Cisco Unified IP Phoneにも適用されます。

安全な電話会議およびセキュリティアイコンの詳細については、お使いの電話機の『管理ガイド』および『*Cisco IP* 電話ユーザガイド』を参照してください。

セキュアな会議 CTI サポート

Unified Communications Manager は、ライセンスを受けた CTI 端末でセキュアな会議をサポートします。 このリリースの『*Unified Communications Manager JTAPI* 開発者ガイド』および『*Unified Communications Manager TAPI* 開発者ガイド』を参照してください。

トランクおよびゲートウェイでのセキュアな電話会議

Unified Communications Manager は、クラスタ内トランク (ICT)、H.323 トランク/ゲートウェイ、MGCP ゲートウェイ経由で安全な電話会議をサポートします。ただし、リリース 8.2 またはそれ以前を実行している暗号化された電話は、ICT および H.323 コールに対して RTP に戻り、メディアは暗号化されません。

電話会議に SIP トランクが含まれる場合、セキュアな電話会議の状況は非セキュアになります。 さらに、SIP トランク シグナリングは、クラスタ外の参加者へのセキュアな会議通知をサポートしていません。

CDR データ

CDR データは、電話会議自体のセキュリティ ステータスだけでなく、電話エンドポイントから電話会議ブリッジまでの各コール レッグのセキュリティ ステータスを提供します。 2 つの値は、CDR データベース内の 2 つの異なるフィールドを使用します。

最低セキュリティレベル要件を満たしていない参加の試みがミートミー電話会議で拒否された場合、CDR データは終了原因コード 58 (ベアラー機能は現在利用できません) を提供します。詳細については、『 *CDR* 分析およびレポート管理ガイド』を参照してください。

連携動作と制限事項

Cisco Unified Communication Manager このセクションには次の項目に関する情報が記載されています:

- Cisco Unified Communications Manager とセキュアな電話会議との相互作用 （176 ページ）
- セキュアな電話会議での Cisco Unified Communications Manager の制限 （177 ページ）

Cisco Unified Communications Manager とセキュアな電話会議との相互作用

この項では、Unified Communications Manager の安全な電話会議機能に関する制限について説明します。

- 電話会議の安全性を維持するために、安全なアドホック電話会議の参加者がコールを保留またはパークした場合、Suppress MOH toConference Bridge サービス パラメータが False に設定されている場合でも、システムはMOHを再生しません。 セキュアな電話会議の状況は変わりません。
- クラスター間環境で、セキュアなアドホック会議でクラスター外の参加者が保留を押すと、デバイスへのメディアストリームが停止し、保留中の音楽が再生され、メディア ステータスが不明に変更されます。 クラスター外の参加者がMOHで保留中の通話を再開すると、電話会議のステータスがアップグレードされる場合があります。
- リモート ユーザがメディア ステータスを不明に変更する電話の機能を起動すると、クラスタ間トランク (ICT) 経由の安全な MeetMe コールが切断されます。
- Unified Communications Manager マルチレベル優先順位と優先権のアナウンス音または通知が、セキュアなアドホック会議中に参加者の端末で再生されると、会議のステータスが非セキュアに変更されます。
- 発信者がセキュアなSCCPコールにバージする場合、システムはターゲットデバイスで内部のトーン再生メカニズムを使用し、ステータスはセキュアなままです。
- 発信者がセキュアなSIP通話に乗り込む場合、システムは保留中の音を提供し、会議の状態は音の間は非セキュアのままとなります。
- 電話会議がセキュアで、RSVP が有効な場合、電話会議はセキュアなままです。
- PSTNが関与する電話会議の場合、セキュリティ電話会議アイコンは通話のIPドメイン部分のみのセキュリティ ステータスを表示します。
- 最大通話継続時間 タイマー サービス パラメータは、電話会議の最大継続時間を制御します。
- 電話会議ブリッジはパケットキャプチャをサポートしています。パケットキャプチャセッション中は、メディアストリームが暗号化されている場合でも、電話会議のノンセキュアステータスが表示されます。
- システムに設定されているメディアセキュリティポリシーにより、安全な電話会議の動作が変わる場合があります。例えば、メディアセキュリティをサポートしていないエンドポイントとの電話会議に参加する場合でも、エンドポイントはシステムのメディアセキュリティポリシーに従ってメディアセキュリティを使用します。

セキュアな電話会議での Cisco Unified Communications Manager の制限

このセクションでは、 Unified Communications Manager の安全な電話会議機能に関する制限について説明します。

- 暗号化された Cisco IP Phone で、リリース 8.2 またはそれ以前を実行しているユーザは、認証された参加者またはセキュアではない参加者としてのみセキュアな電話会議に参加することができます。

- リリース 8.3 以前のリリースを使用している Unified Communications Manager で動作する Cisco Unified IP Phone は、接続のセキュリティステータスを表示し、会議のセキュリティステータスではない。会議リストのようなセキュアな会議機能はサポートしていません。
- Cisco Unified IP Phone 7800 および 7911G はリスト会議をサポートしていません。
- 帯域幅の要件により、 Cisco Unified IP Phone 7942 および 7962 はアクティブな暗号化コールでの暗号化デバイスからの割り込みをサポートしていません。割り込みの試みは失敗します。
- Cisco Unified IP Phone 7931G は会議の連鎖に対応していません。
- SIP トランク経由で発信している電話は、デバイスのセキュリティ ステータスに関係なく、セキュアではない電話として扱われます。
- セキュアな電話が SIP トランク経由でセキュアな Meet-Me 電話会議に参加しようとすると、コールがドロップされます。 SIP トランクは、SIP を実行している電話への 「デバイスは認証されていません」 メッセージの提供をサポートしていないため、電話はこのメッセージで更新されません。 さらに、SIP を実行している 7962 電話は 「端末は認証されていません」 メッセージをサポートしていません。
- クラスター間環境では、電話会議リストにはクラスター外の参加者は表示されません。ただし、クラスタ間の接続でサポートされている限り、接続のセキュリティ ステータスは [電話会議] ソフトキーのとなりに表示されます。 たとえば、H.323 ICT 接続の場合、認証アイコンは表示されませんが、システムは認証された接続をセキュアではないものとして扱います。しかし暗号化された接続の場合は暗号化アイコンが表示されます。

  クラスター外の参加者は、クラスターの境界を越えて別のクラスターに接続する独自の電話会議を作成できます。 システムは、接続済みの電話会議を、2 者間での基本的なコールとして扱います。

電話会議リソースを保護するためのヒント

セキュアな会議ブリッジリソースを構成する前に、以下の情報を考慮してください。

- 電話会議のメッセージでカスタムテキストを表示させる場合は、ローカリゼーションを使用します。 詳細については、Unified Communications Manager ロケールインストーラのドキュメントを参照してください。
- 電話会議または内蔵ブリッジは、セキュアな電話会議をサポートするために暗号化が必要です。
- 安全な電話会議ブリッジ登録を有効にするには、クラスタセキュリティモードを混合モードに設定します。
- 電話会議を開始する電話が認証済みまたは暗号化されており、セキュアな電話会議ブリッジを得ることを確認してください。

- 共有回線で電話会議の整合性を維持するために、異なるセキュリティモードで回線を共有するデバイスを設定しないでください。たとえば、暗号化された電話を、認証された電話や保護されていない電話と回線を共有するように設定しないでください。
- クラスタ間で電話会議のセキュリティ ステータスを共有する場合は、SIP トランクを ICT として使用しないでください。
- クラスタセキュリティモードを混合モードに設定する場合、DSP ファームに設定されているセキュリティモード（非セキュアまたは暗号化）は、Unified Communications Manager Administration での電話会議ブリッジのセキュリティモードと一致していなければ、電話会議ブリッジは登録できません。 両方のセキュリティモードで暗号化が指定されている場合、電話会議ブリッジは暗号化済みとして登録します。両方のセキュリティモードで非セキュアが指定されている場合、会議ブリッジは非セキュアとして登録されます。
- クラスタセキュリティモードを混合モードに設定し、電話会議ブリッジに適用したセキュリティプロファイルが暗号化されているものの、電話会議ブリッジのセキュリティレベルがセキュアではない場合、Unified Communications Manager は、電話会議ブリッジの登録を拒否します。
- クラスタ セキュリティ モードをノンセキュア モードに設定する場合、DSP ファームでセキュリティモードをノンセキュアとして設定し、これにより会議ブリッジが登録できるようになります。 Unified Communications Manager Administration の設定で暗号化が指定されている場合でも、電話会議ブリッジがノンセキュアとして登録されます。
- 登録時に、電話会議ブリッジは認証に合格する必要があります。 認証に合格するには、DSP ファームには Unified Communications Manager の証明書が、また Unified Communications Manager には DSP ファームシステムと DSP 接続の証明書が含まれている必要があります。電話会議ブリッジが認証にパスすることを確認するには、X509 証明書の名前に電話会議ブリッジの名前が含まれている必要があります。

ヒント　会議ブリッジ名が一意であること、および[デバイス]テーブルの下の他の場所で設定できないことを確認します。 これは、ルートリスト、SIP トランク、IP 電話などに適用されます。

- Cisco Unity 証明書の有効期限が切れたり、何らかの理由で変更されたりした場合は、『Cisco Unified Communications オペレーティング システム アドミニストレーション ガイド』の証明書管理機能を使用して、信頼できるストアの証明書を更新してください。 証明書が一致しない場合、TLS 認証は失敗します。また、電話会議ブリッジは Unified Communications Manager に登録できないため、機能しません。
- セキュアな会議ブリッジは、ポート 2443 の TLS 接続を介して Unified Communications Manager に登録します。セキュアではない会議ブリッジが、ポート 2000 の TCP 接続を介して Unified Communications Manager に登録します。
- コンファレンスブリッジのデバイスセキュリティモードを変更するには、Unified Communications Manager デバイスをリセットし、Cisco CallManager サービスを再起動する必要があります。

セキュアな電話会議ブリッジのセットアップ

以下の手順は、ネットワークに安全な電話会議を追加するために使用されるタスクを提供します。

手順

ステップ 1 混合モード用の CiscoCTL クライアントがインストールされ、構成されていることを確認します。

ステップ 2 Unified Communications Manager 接続用の DSP ファームのセキュリティ設定を確認します。これには、 Unified Communications Manager の証明書をトラストストアに追加することも含まれます。 DSP ファームのセキュリティ レベルを暗号化に設定します。

お使いの電話会議ブリッジのドキュメントを参照してください。

ヒント
DSP ファームは、 Unified Communications Manager への TLS ポート接続をポート 2443 で確立します。

ステップ 3 DSP ファーム証明書が CallManager 信頼ストアにあることを確認します。

証明書を追加するには、 Cisco Unified Communications オペレーティングシステム の証明書管理機能を使用して、DSP 証明書を Unified Communications Managerの信頼できるストアにコピーします。

証明書のコピーが完了したら、サーバ上の CiscoCallManager サービスを再起動してください。

詳細については、『*Cisco Unified Communications Manager* アドミニストレーションガイド』および『*Cisco Unified Serviceability* アドミニストレーションガイド』を参照してください。

ヒント
クラスタの各サーバに証明書をコピーし、クラスタの各サーバで CiscoCallManager サービスを再起動してください。

ステップ 4 Unified Communications Manager Administration で、会議ブリッジタイプとして Cisco IOS Enhanced 会議ブリッジを設定し、デバイスセキュリティモードに暗号化会議ブリッジを選択します。

ヒント
このリリースにアップグレードすると、 Unified Communications Manager が自動的に非セキュア会議ブリッジセキュリティプロファイルを Cisco IOS Enhanced 会議ブリッジ構成に割り当てます。

ステップ 5 ミートミー電話会議の最低セキュリティレベルを設定します。

ヒント
このリリースにアップグレードする際、 Unified Communications Manager は自動的に非セキュアの最小セキュリティレベルをすべての Meet Me パターンに割り当てます。

ステップ 6 セキュアな電話会議ブリッジのパケットキャプチャを設定します。

詳細については、『トラブルシューティングガイド*Cisco Unified Communications Manager* トラブルシューティングガイド』を参照してください。

ヒント
パケット キャプチャ モードをバッチ モードに設定し、キャプチャ層を SRTP に設定します。

Cisco Unified Communications Manager Administration でセキュアな電話会議ブリッジをセットアップする

Unified Communications Manager Administration でセキュアな電話会議を設定するには、次の手順を実行します。 コンファレンスブリッジの暗号化を設定したら、Unified Communications Manager デバイスをリセットし、CiscoCallManager サービスを再起動する必要があります。

デバイス間の接続をセキュリティ保護するために、Unified Communications Manager と DSP ファームに証明書がインストールされていることを確認してください。

始める前に

事前準備

手順

ステップ 1 **[メディアリソース（Media Resources）]**>**[会議ブリッジ（Conference Bridge）]** を選択します。

ステップ 2 [**会議ブリッジの検索と一覧表示**] ウィンドウで、Cisco IOS Enhanced Conference Bridgeがインストールされていることを確認し、次に移動しますセキュアな電話会議ブリッジのセットアップ （180 ページ）。

ステップ 3 端末がデータベースに存在しない場合は、**[新規追加（Add New）]** をクリックし、Cisco Unified Communications Manager Administration でセキュアな電話会議ブリッジをセットアップする （181 ページ） に進みます。

ステップ 4 [電話会議ブリッジの設定] ウィンドウで、[**電話会議ブリッジタイプ**] ドロップダウンリストから **Cisco IOS Enhanced 会議ブリッジ** を選択します。『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の説明に従って、[電話会議ブリッジの名前]、[説明]、[デバイスプール]、[共通のデバイス構成]、[ロケーション] の設定を行います。

ステップ 5 [端末のセキュリティモード] フィールドで [**暗号化会議ブリッジ**] を選択します。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 [**リセット（Reset）**] をクリックします。

次のタスク

追加の会議ブリッジ設定タスクを実行するには、[ミートミー/番号パターンの設定] ウィンドウまたは [サービスパラメータの設定] ウィンドウに移動できます。これを行うには、[関連リンク] ドロップダウンリストボックスからオプションを選択し、[実行] をクリックします。

ミートミー電話会議の最低セキュリティレベルのセットアップ

ミートミー電話会議の最低セキュリティレベルを設定するには、次の手順を実行します。

手順

ステップ 1 [**通話ルーティング** >] **ミートミー番号/パターンを選択します。**

ステップ 2 [電話会議ブリッジの検索と一覧表示] ウィンドウで、ミートミー番号/パターンが設定されていることを確認し、セキュアな電話会議ブリッジのセットアップ（180 ページ） に移動します。

ステップ 3 ミートミー番号/パターンが設定されていない場合は、**新規追加** をクリックします。ミートミー電話会議の最低セキュリティレベルのセットアップ（182 ページ） に移動してください。

ステップ 4 [**Meet-Me番号設定**] ウィンドウの [ディレクトリ番号またはパターン] フィールドに、Meet-Me 番号または範囲を入力します。『*Cisco Unified Communications Manager* 機能設定ガイド』の説明に従って、説明とパーティションを設定します。

ステップ 5 [最小セキュリティレベル（Minimum Security Level）] フィールドで、**[セキュリティ保護なし（Non Secure）]**、**[認証あり（Authenticated）]**、または **[暗号化（Encrypted）]** を選択します。

ステップ 6 **[保存（Save）]** をクリックします。

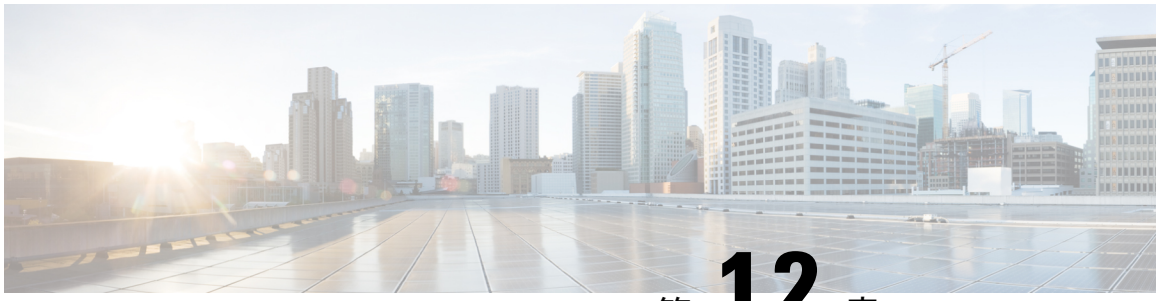
次のタスク

セキュアな会議ブリッジをまだインストールしていない場合は、セキュアな会議ブリッジをインストールして設定します。

セキュアな電話会議用のパケットキャプチャのセットアップ

セキュアな会議ブリッジのパケットキャプチャを設定するには、[**サービスパラメータ設定**] ウィンドウでパケットキャプチャを有効にします。次に、デバイス構成ウィンドウで、電話、ゲートウェイ、またはトランクに対して、パケット キャプチャ モードをバッチ モードに設定し、キャプチャ層を SRTP に設定します。 詳細については、『 トラブルシューティングガイド*Cisco Unified Communications Manager* トラブルシューティングガイド』を参照してください。

パケット キャプチャ セッション中は、メディア ストリームが暗号化されている場合でも、電話会議のノンセキュア ステータスが表示されます。



第 12 章

ボイスメッセージ ポートのセキュリティ設定

この章では、ボイスメッセージ ポートのセキュリティ設定について説明します。

- ボイスメッセージのセキュリティ （185 ページ）
- ボイスメッセージのセキュリティ設定のヒント （186 ページ）
- セキュアなボイスメッセージ ポートのセットアップ （187 ページ）
- 単一のボイスメッセージ ポートへのセキュリティ プロファイルの適用 （188 ページ）
- ボイスメールポートウィザードを使用してセキュリティプロファイルを適用 （188ページ）

ボイスメッセージのセキュリティ

Unified Communications Managerのボイスメッセージングポートと、SCCPを実行しているCisco Unityデバイスまたは SCCPを実行しているCisco Unity Connectionデバイスのセキュリティを設定するには、ポートのセキュアなデバイスセキュリティモードを選択します。 認証済みのボイスメール ポートを選択した場合、TLS 接続が開き、相互証明書交換を使用してデバイスを認証します (各デバイスは他のデバイスの証明書を受け入れます)。 暗号化されたボイスメール ポートを選択した場合、システムはまずデバイスを認証し、それからデバイス間で暗号化された音声ストリームを送信します。

Cisco Unity Connection は TLS ポート経由で Unified Communications Manager に接続します。 デバイスのセキュリティモードがノンセキュアの場合、 Cisco Unity Connection は SCCP ポート経由で Unified Communications Manager に接続します。

（注） この章で使用する「 「サーバ」 」という用語は、「 Unified Communications Manager サーバ」を指します。 「 「ボイスメールサーバ」 」という語句は、 Cisco Unity サーバまたは Cisco Unity Connection サーバを指します。

ボイスメッセージのセキュリティ設定のヒント

セキュリティを設定する前に、以下の情報を考慮してください。

- Cisco Unity の場合、 Cisco Unity テレフォニーインテグレーションマネージャ (UTIM) を使用してセキュリティタスクを実行する必要があります。 Cisco Unity Connection については、 Cisco Unity Connection 管理 を使用してセキュリティタスクを実行する必要があります。 これらのタスクの実行方法の詳細については、『Unified Communications Manager インテグレーションガイド』（Cisco Unity 向け）または Cisco Unity Connection向け』を参照してください。
- この章で説明する手順に加えて、Unified Communications Manager の証明書管理機能を使用して、Cisco Unity 証明書を信頼できるストアに保存します。

  詳細については、次のURLにある『「Cisco Unity Connection 管理でボイスメッセージングポートを追加する』」 手順を含む *Cisco Unity*用*Cisco Unified Communications Manager SCCP* インテグレーションガイド を参照してください。

  http://www.cisco.com/en/US/docs/voice_ip_comm/connection/10x/integration/guide/cucm_sccp/guide/cucintcucmskinny230.html

  証明書をコピーしたら、クラスタ内の各 Unified Communications Manager サーバで CiscoCallManager サービスを再起動する必要があります。
- Cisco Unity 証明書の有効期限が切れたり、何らかの理由で変更されたりした場合は、『*Cisco Unified Communications Manager* アドミニストレーションガイド』の証明書管理機能を使用して、信頼できるストアの証明書を更新してください。 証明書が一致しない場合、TLS 認証は失敗し、 Unified Communications Manager に登録できないため、ボイスメッセージが機能しません。
- ボイスメール サーバ ポートを構成するとき、デバイス セキュリティ モードを選択する必要があります。
- Cisco Unity テレフォニー統合マネージャ (UTIM) または Cisco Unity Connection 管理 で指定する設定は、必ず Unified Communications Manager Administrationで設定したボイスメッセージポート端末のセキュリティモードと一致させてください。 Cisco Unity Connection 管理の [ボイスメールポートの設定] ウィンドウ (または [ボイスメールポートウィザード]) でボイスメッセージポートにデバイスセキュリティモードを適用します。

ヒント デバイスのセキュリティモード設定が一致しない場合、ボイスメールサーバのポートはUnified Communications Manager に登録されず、ボイスメールサーバはこれらのポートでの通話を受け付けることができません。

- ポートのセキュリティプロファイルを変更するには、 Unified Communications Manager 端末をリセットし、ボイスメールサーバソフトウェアを再起動する必要があります。 Unified Communications Manager Administration で以前のプロファイルとは異なるデバイスセキュリ

ティモードを使用するセキュリティプロファイルを適用する場合、ボイスメールサーバの設定を変更する必要があります。

- ボイスメール ポート ウィザードを使用して、既存のボイスメール サーバのデバイス セキュリティ モードを変更することはできません。 既存のボイスメール サーバにポートを追加する場合、プロファイルに現在設定されているデバイス セキュリティ モードが自動的に新しいポートに適用されます。

セキュアなボイスメッセージ ポートのセットアップ

次の手順では、ボイスメッセージ ポートのセキュリティを設定するための作業を示します。

手順

ステップ 1 混合モード用の CiscoCTL クライアントがインストールされ、構成されていることを確認します。

ステップ 2 電話で認証または暗号化を設定したことを確認します。

ステップ 3 Cisco Unified Communications Operating System Administration の証明書管理機能を使用して、Cisco Unity 証明書を Unified Communications Manager サーバーの信頼できるストアにコピーし、CiscoCallManager サービスを再起動します。

詳細については、『*Cisco Unified Communications Manager* アドミニストレーションガイド』および『*Cisco Unified Serviceability* アドミニストレーションガイド』を参照してください。

ヒント
クラスタ内の各 Unified Communications Manager サーバーで Cisco CTL Provider サービスを有効にします。その後、すべてのサーバー上で Cisco CallManager サービスを再起動します。

ステップ 4 Unified Communications Manager Administration で、ボイスメッセージポートのデバイスセキュリティモードを設定します。

ステップ 5 Cisco Unity または Cisco Unity Connection ボイスメッセージポートのセキュリティ関連の設定タスクを実行します。例えば、Cisco Unity をCisco TFTP サーバーを指すように設定します。

Cisco Unity または Cisco Unity Connection についての詳細は、『*Unified Communications Manager* インテグレーションガイド』を参照してください。

ステップ 6 Unified Communications Manager Administration で端末をリセットし、 Cisco Unity ソフトウェアを再起動してください。

Cisco Unity または Cisco Unity Connection についての詳細は、『*Unified Communications Manager* インテグレーションガイド』を参照してください。

単一のボイスメッセージ ポートへのセキュリティ プロファイルの適用

単一のボイスメッセージポートにセキュリティプロファイルを適用するには、次の手順を実行します。

この手順は、デバイスがデータベースに追加され、電話機に証明書がインストールされていることを前提としています (証明書がまだ存在していない場合)。 初めてセキュリティ プロファイルを適用した場合、またはセキュリティプロファイルを変更した場合は、デバイスをリセットする必要があります。

始める前に

セキュリティプロファイルを適用する前に、ボイスメッセージのセキュリティと安全なボイスメッセージポートの設定に関するトピックを見直してください。

手順

ステップ 1 『*Cisco Unified Communications Manager* アドミニストレーションガイド』の説明に従って、ボイスメッセージポートを見つけます。

ステップ 2 ポートの設定ウィンドウが表示されたら、**端末セキュリティモード**（**Device Security Mode**）設定を見つけます。 ドロップダウン リスト ボックスから、ポートに適用するセキュリティモードを選択します。 このオプションは、データベースで事前定義されています。 デフォルトでは **未選択**となっています。

ステップ 3 **[保存（Save）]** をクリックします。

ステップ 4 [**リセット**（**Reset**）] をクリックします。

ボイスメールポートウィザードを使用してセキュリティプロファイルを適用

この手順を使用して、ボイスメールポートウィザードで新しいボイスメールサーバにデバイスセキュリティモード設定を適用します。

既存のボイスメールサーバのセキュリティ設定を変更するには、単一のボイスメッセージポートへのセキュリティプロファイルの適用に関するトピックを参照してください。

始める前に

セキュリティプロファイルを適用する前に、ボイスメッセージのセキュリティと安全なボイスメッセージポートの設定に関するトピックを見直してください。

手順

ステップ 1 Unified Communications Manager Administration から、 **ボイスメール** > **Cisco ボイスメールポートウィザードを選択します**。

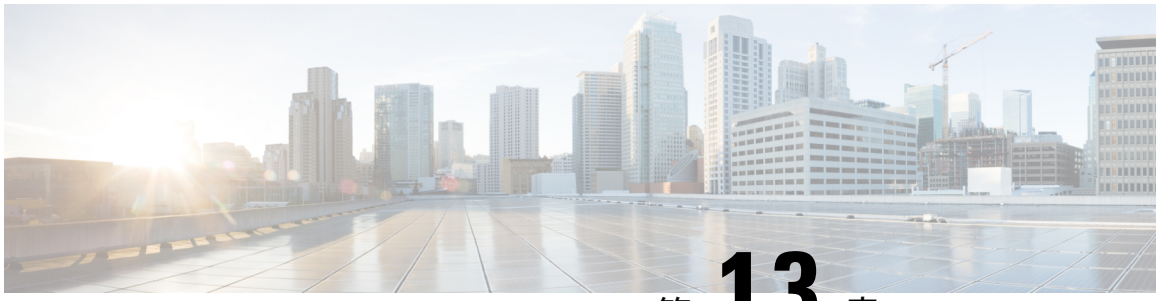
ステップ 2 ボイスメールサーバの名前を入力します。[**次へ**] をクリックします。

ステップ 3 追加するポートの数を選択します。[**次へ**] をクリックします。

ステップ 4 **Cisco ボイスメール端末情報** ウィンドウで、ドロップダウンリストボックスから **端末セキュリティモード** を選択します。このオプションは、データベースで事前定義されています。デフォルトでは **未選択** となっています。

ステップ 5 その他のデバイス設定を行います。詳細は、『*Cisco Unified Communications Manager* アドミニストレーションガイド』に従ってください。 [次へ（Next）]をクリックします。

ステップ 6 『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の説明に従って、設定を続行します。 **サマリー** ウィンドウが表示されたら、 **終了** をクリックします。



第 13 章

トランクおよびゲートウェイ SIP セキュリティ

- トランクおよびゲートウェイ SIP セキュリティの概要 （191 ページ）
- トランクとゲートウェイの SIP セキュリティ タスク フローの設定 （196 ページ）

トランクおよびゲートウェイ SIP セキュリティの概要

このセクションでは、SIP トランク暗号化、ゲートウェイ暗号化、およびセキュリティプロファイル設定のヒントの概要について説明します。

SIP トランク暗号化

SIP トランクは、シグナリングとメディアの両方でセキュアなコールをサポートできます。TLS はシグナリングの暗号化を提供し、SRTP はメディアの暗号化を提供します。

トランクのシグナリング暗号化を設定するには、SIP トランク セキュリティ プロファイル (**システム** > **セキュリティ プロファイル** > **SIP トランク セキュリティ) を設定するときに次のオプションを選択します。プロファイル** ウィンドウ。

- **端末のセキュリティモード** ドロップダウンリストから 「暗号化を選択します。」
- **受信トランスポートタイプ** ドロップダウンリストから 「TLS を選択します。」
- **発信トランスポートタイプ** ドロップダウンリストから 「TLS を選択します。」

SIP トランクセキュリティプロファイルを設定したら、それをトランクに適用します（ **端末** > **トランク** > **SIP トランク** 設定ウィンドウ）。

トランクのメディア暗号化を設定するには、[**SRTP 許可**] チェックボックスを選択します (**端末トランクSIP トランク** 設定ウィンドウ)。

注意 このチェックボックスをオンにする場合、暗号化された TLS プロファイルを使用して、キーおよび他のセキュリティ関連情報が通話ネゴシエーション中に露出しないようにすることを推奨します。 安全ではないプロファイルを使用する場合、SRTP は引き続き機能しますが、キーはシグナリングとトレースで公開されます。 この場合、Unified Communications Manager とトランクの接続先の間でネットワークのセキュリティを確保する必要があります。

Cisco IOS MGCP ゲートウェイ暗号化

Unified Communications Manager は、セキュアな RTP 接続でパケットを暗号化および復号化するために使用される MGCP SRTP パッケージを使用するゲートウェイをサポートします。 通話のセットアップ中に交換される情報によって、ゲートウェイが通話に SRTP を使用するかどうかが決まります。 デバイスが SRTP をサポートしている場合、システムは SRTP 接続を使用します。 1 つ以上のデバイスが SRTP をサポートしていない場合、システムは RTP 接続を使用します。 SRTP から RTP へのフォールバック (およびその逆) は、セキュアなデバイスからセキュアではないデバイスへの転送、電話会議、トランスコーディング、保留音などで発生する可能性があります。

それが2台の端末間のSRTP通話の暗号化をセットアップする際、 Unified Communications Manager マスター暗号化キーとSaltを生成して通話をセキュアなものにし、SRTPストリームの場合にのみゲートウェイに送信します。 Unified Communications Manager それはゲートウェイもサポートしているSRTCPストリームのキーとSaltを送信しません。 これらのキーは、IPSec を使用してセキュリティ保護する必要がある、MGCP シグナリング パスを介してゲートウェイに送信されます。 Unified Communications Manager それはIPSec接続が存在するかどうかを認識しませんが、IPSecが構成されていない場合、システムはセッションキーをクリアテキストでゲートウェイに送信します。 あなたはIPSec接続が確立されていることを確認します。セッションキーは安全な接続で送信されます。

ヒント それがSRTP用に設定されたMGCPゲートウェイが、SCCPを実行している認証された電話機など、認証されたデバイスとのコールに関連している場合、盾のアイコンが電話機に表示されます。 Unified Communications Manager それは、デバイスのSRTP機能が通話に対して正常にネゴシエートされた場合に、通話を暗号化として分類します。 Unified Communications Manager セキュリティ アイコンを表示できる電話機に MGCP ゲートウェイが接続されている場合、コールが暗号化されると、電話機にはロック アイコンが表示されます。

以下は、MGCP E1 PRI ゲートウェイに関する事実です。

- SRTP 暗号化の MGCP ゲートウェイを設定する必要があります。 次のコマンドを使用してゲートウェイを設定します: **mgcppackage-capabilitysrtp-package**
- MGCP ゲートウェイは、Advanced IP Services または Advanced Enterprise Services のイメージを指定する必要があります。

  例: **c3745-adventerprisek9-mz.124-6.T.bin**

- Protected ステータスは、MGCP PRI セットアップ、アラート、および接続メッセージで独自の FacilityIE を使用することで、MGCP E1 PRI ゲートウェイと交換されます。
- Unified Communications Manager がセキュアな通知トーンを再生するのは Cisco Unified IP 電話だけです。 ネットワーク内の PBX は、通話のゲートウェイ側に対してトーンを再生します。
- Cisco Unified IP Phone と MGCP E1 PRI ゲートウェイの間のメディアが暗号化されていない場合、コールはドロップされます。

（注） MGCP ゲートウェイの暗号化の詳細については、お使いのバージョンの Cisco IOS ソフトウェアに対応する *Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways* を参照してください。

H.323 ゲートウェイおよび H.323/H.225/H.245 トランク暗号化

セキュリティをサポートする H.323 ゲートウェイおよびゲートキーパーまたはゲートキーパーではない H.225/H.323/H.245 トランクは、Cisco Unified Communications Operating System 内で IPSec の関連付けを設定した場合、Unified Communications Manager に対して認証を行うことができます。 Unified Communications Manager とこれらの端末間の IPSec 関連付けの作成については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』』を参照してください。

H.323、H.225、H.245 デバイスは暗号化キーを生成します。 これらのキーは、シグナリングパスを通じて Unified Communications Manager に送信されます。シグナリングパスは IPSec で保護します。 Unified Communications Manager は IPSec 接続が存在するかどうかを認識しませんが、IPSec が設定されていない場合、セッションキーはプレーンテキストで送信されます。IPSec接続が確立されていることを確認します。セッションキーは安全な接続で送信されます。

IPSec 関連付けの設定に加えて、 Unified Communications Manager Administrationのデバイス設定ウィンドウで [SRTP 許可] チェックボックスをオンにする必要があります。たとえば、H.323 ゲートウェイ、H.225 トランク (ゲートキーパー制御)、クラスター間トランク (ゲートキーパー制御)、クラスター間トランク (非ゲートキーパー制御) 構成ウィンドウなどです。 このチェックボックスをオフにすると、 Unified Communications Manager は RTP を使用してデバイスと通信します。 チェックボックスをオンにすると、 Unified Communications Manager でセキュアおよび非セキュアの通話が可能になります。これは、端末に SRTP が設定されているかどうかによって異なります。

注意 Unified Communications Manager Administration で [SRTP 許可] チェックボックスをオンにする場合、Cisco では IPSec を設定して、セキュリティ関連情報がクリアテキストで送信されないようにすることを強く推奨します。

Unified Communications Manager は、ユーザが IPSec 接続を正しく設定したかどうかを確認しません。接続を適切に構成しないと、セキュリティ関連情報が暗号化されずに送信される場合があります。

システムがセキュアなメディアまたはシグナリングパスを確立でき、デバイスが SRTP をサポートしている場合、システムは SRTP 接続を使用します。システムがセキュアなメディアまたはシグナリングパスを確立できない場合、または少なくとも 1 つのデバイスが SRTP をサポートしていない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバック (およびその逆) は、セキュアなデバイスからセキュアではないデバイスへの転送、電話会議、トランスコーディング、保留音などで発生する可能性があります。

ヒント 通話でパススルー対応 MTP が使用され、地域フィルタリング後にデバイスの音声機能が一致し、どのデバイスに対しても [MTP が必要] チェックボックスが選択されていない場合、Unified Communications Manager は通話をセキュアなものに分類します。 [MTP が必要] チェックボックスがオンの場合、 Unified Communications Manager は通話の音声パススルーを無効にし、通話はノンセキュアとして分類されます。 通話に MTP が含まれていない場合、 Unified Communications Manager は、端末の SRTP 機能に応じて通話を暗号化通話として分類する場合があります。

SRTP が設定されたデバイスの場合、[SRTP を許可する（ SRTP Allowed）] チェックボックスがデバイスに対して有効であり、デバイスの SRTP 機能のネゴシエートに成功すると、Unified Communications Manager は通話を暗号化通話として分類します。 上記の条件が満たされない場合、 Unified Communications Manager は通話をセキュリティ保護されていないものとして分類します。 セキュリティ アイコンを表示できる電話にデバイスが接続されている場合、通話が暗号化されると、電話にロック アイコンが表示されます。

Unified Communications Manager は、トランクまたはゲートウェイを介した発信のファストスタート通話を非セキュアとして分類します。 Unified Communications Manager Administration で [SRTP 許可（SRTP Allowed）] チェックボックスをオンにすると、Unified Communications Manager は **[アウトバウンド FastStart を有効にする（Enable Outbound FastStart）]** チェックボックスを無効にします。

Unified Communications Manager では、ゲートウェイとトランクの種類によっては、2 つの H.235 エンドポイント間で共有秘密（Diffie-Hellman キー）とその他の H.235 データを透過的にパススルーさせることができるため、2 つのエンドポイント間でセキュアなメディアチャネルを確立できます。

H.235 データのパススルーを有効にするには、次のトランクとゲートウェイの構成設定で **H.235 パススルーの許可** チェックボックスを選択します:

- H.225 トランク

- ICT ゲートキーパーコントロール
- ICT 非ゲートキーパーコントロール
- H.323 ゲートウェイ

トランクとゲートウェイの設定については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』を参照してください。

SIP トランク セキュリティ プロファイルの設定について

Unified Communications Manager Administrationでは、SIP トランクに対するセキュリティ関連の設定がグループ化され、1 つのセキュリティプロファイルを複数の SIP トランクに割り当てることができます。セキュリティに関連する設定には、デバイスセキュリティモード、ダイジェスト認証、および着信/発信転送タイプの設定があります。 設定した値を SIP トランクに適用するには、**トランクの設定(Trunk Configuration)**ウィンドウでセキュリティ プロファイルを選択します。

Unified Communications Manager をインストールすると、自動登録用の事前定義済み非セキュア SIP トランク セキュリティ プロファイルが提供されます。 SIP トランクのセキュリティ機能を有効にするには、新しいセキュリティプロファイルを設定し、SIP トランクに適用します。 トランクがセキュリティをサポートしていない場合は、非セキュアプロファイルを選択します。

SIP トランクがサポートするセキュリティ機能だけが、セキュリティ プロファイル設定ウィンドウに表示されます。

SIP トランク セキュリティ プロファイルのセットアップのヒント

Unified Communications Manager Administration で SIP トランクセキュリティプロファイルを設定する場合は、以下の情報を考慮してください:

- SIP トランクを設定する場合、[トランク設定] ウィンドウでセキュリティ プロファイルを選択する必要があります。デバイスがセキュリティをサポートしていない場合、非セキュア プロファイルを適用します。
- 現在デバイスに割り当てられているセキュリティプロファイルを削除することはできません。
- すでにSIP トランクに割り当てられているセキュリティプロファイルの設定を変更する場合、再設定した設定は、そのプロファイルが割り当てられているすべての SIP トランクに適用されます。
- デバイスに割り当てられているセキュリティファイルの名前を変更することができます。古いプロファイル名と設定が割り当てられている SIP トランクは、新しいプロファイル名と設定を引き継ぎます。
- Unified Communications Manager 5.0 以降にアップグレードする前にデバイスセキュリティモードを設定した場合、Unified Communications Manager は SIP トランクのプロファイルを作成し、プロファイルをデバイスに適用します。

トランクとゲートウェイの SIP セキュリティ タスク フローの設定

以下のタスクを完了してゲートウェイと SIP のセキュリティを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	セキュアなゲートウェイとトランクのセットアップ	セキュリティのためにセキュアなゲートウェイとトランクを有効にします。
ステップ 2	SIP トランク セキュリティ プロファイルのセットアップ	SIP トランク セキュリティ プロファイルを追加、更新、またはコピーします。
ステップ 3	SIP トランク セキュリティ プロファイルの適用	SIP トランク セキュリティ プロファイルをトランクに適用し、有効にします。セキュリティ プロファイルをデバイスに適用します。
ステップ 4	SIP トランクと SIP トランク セキュリティ プロファイルを同期する	SIP トランクを SIP トランク セキュリティ プロファイルと同期させます。
ステップ 5	Unified Communications Manager Administration を使用して SRTP を許可する	H.323 ゲートウェイおよびゲートキーパーまたは非ゲートキーパーで制御される H.323/H.245/H.225 トランクまたは SIP トランクの SRTP Allowed オプションを設定します。

セキュアなゲートウェイとトランクのセットアップ

この手順は、ドキュメント *Media andSignaling Authentication and EncryptionFeature for Cisco IOS MGCP Gateways*と併せて使用してください。このドキュメントには、セキュリティのために Cisco IOS MGCP ゲートウェイを設定する方法が記載されています。

手順

ステップ 1 **utils ctl** コマンドを実行してクラスタを混合モードに設定したことを確認してください。

ステップ 2 電話で暗号化を設定したことを確認してください。

ステップ 3 IPSec を設定します。

ヒント

ネットワークインフラにIPSecを設定するか、 Unified Communications Manager とゲートウェイやトランク間でIPSecを設定できますよ。 一方の方法を実装して IPSec をセットアップする場合、もう一方の方法を実装する必要はありません。

ステップ 4 H.323 IOS ゲートウェイおよびクラスタ間トランクの場合、 で SRTP 許可 チェックボックスを選択します。 Unified Communications Manager

SRTP 許可 チェックボックスが **トランク構成** または **ゲートウェイ構成** ウィンドウに表示されます。 これらのウィンドウの表示方法に関する情報は、Cisco Unified Communications Manager アドミニストレーション ガイドのトランクとゲートウェイの章を参照してください。

ステップ 5 SIP トランクの場合、SIP トランク セキュリティ プロファイルを設定し、トランクに適用します (まだ実行していない場合)。 また、必ず **Device** Trunk **SIP Trunk Configuration** > **ウィンドウの** > **SRTP 許可** チェックボックスをオンにしてください。

注意
SRTP 許可 チェックボックスを選択する場合は、暗号化された TLS プロファイルを使用することを推奨します。これにより、通話ネゴシエーション中に鍵やその他のセキュリティ関連情報が漏洩しないようにします。 安全ではないプロファイルを使用する場合、SRTP は引き続き機能しますが、キーはシグナリングとトレースで公開されます。 この場合、Unified Communications Manager とトランクの接続先の間でネットワークのセキュリティを確保する必要があります。

ステップ 6 ゲートウェイでセキュリティ関連の設定タスクを実行します。

詳細については、 *Cisco IOS MGCP* ゲートウェイのメディアおよびシグナリングの認証と暗号化機能を参照してください。

SIP トランク セキュリティ プロファイルのセットアップ

SIP トランクセキュリティプロファイルを追加、更新、またはコピーするには、以下の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから **システム** > **セキュリティプロファイル** > **SIP トランクセキュリティプロファイル**を選択します。

ステップ 2 次のいずれかの作業を実行します。

a) 新しい CAPF プロファイルを追加するには、**[検索対象（Find）]** ウィンドウで **[新規追加]** をクリックします。

(プロファイルを表示して、[**新規追加**] をクリックすることもできます。)

設定ウィンドウには、各フィールドの既定の設定が表示されます。

b) 既存のプロファイルをコピーするには、適切なプロファイルを見つけ、[コピー（Copy）] 列内にあるそのレコード用の **[コピー（Copy）]** アイコンをクリックします

(プロファイルを表示して [**コピー**] をクリックすることもできます。)

構成ウィンドウに構成済みの設定が表示されます。

c) 既存のプロファイルを更新するには、SIP トランク セキュリティ プロファイルの検索 で説明されているように、適切なセキュリティプロファイルを見つけて表示します。

[権限の設定(Role Configuration)] ウィンドウが表示され、現在の設定が表示されます。

ステップ 3 SIP トランク セキュリティ プロファイル設定の説明に従って、適切な設定を入力します。

ステップ 4 **[保存（Save）]** をクリックします。

セキュリティプロファイルを作成したら、トランクに適用します。 SIP トランクのダイジェスト認証を設定した場合、まだ行っていない場合は、トランクの **SIP Realm** ウィンドウと、SIP トランクを介して接続されるアプリケーションの **アプリケーションユーザ** ウィンドウでダイジェスト認証情報を設定する必要があります。 SIP トランクを介して接続されるアプリケーションに対してアプリケーションレベルの認証を有効にした場合、まだ行っていない場合は、アプリケーションに許可する認証方法を **アプリケーションユーザ** ウィンドウで設定する必要があります。

SIP トランク セキュリティ プロファイルの設定項目

次の表に、SIP トランク セキュリティ プロファイルの設定項目の説明を示します。

表 *30 : SIP* トランク セキュリティ プロファイルの設定項目

設定	説明
名前	セキュリティ プロファイルの名前を入力します。 新しいプロファイルを保存すると、[Trunk Configuration] ウィンドウの [SIP Trunk Security Profile] ドロップダウン リスト ボックスにその名前が表示されます。
説明	セキュリティ プロファイルの説明を入力します。 説明には、どの言語でも最大 50 文字まで指定できますが、二重引用符（"）、パーセント記号（%）、アンパサンド（&）、バックスラッシュ（\）、山カッコ（<>）は使用できません。

設定	説明
[デバイスセキュリティモード(Device Security Mode)]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • **[非セキュア(Non Secure)]**：イメージ認証以外のセキュリティ機能を適用しません。 TCP または UDP 接続で Unified Communications Manager が利用できます。 • **認証（Authenticated**）: Unified Communications Manager はトランクの整合性と認証を提供します。 NULL/SHA を使用する TLS 接続を開始します。 • **暗号化（Encrypted**）: Unified Communications Managerはトランクの整合性、シグナリング、および認証を提供します。 シグナリング用に、AES128/SHA を使用する TLS 接続を開始します。 （注） **認証済み**として選択されている [デバイスのセキュリティプロファイル (トランク)] を使用して設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS connection (データ暗号化なし) を開始します。 これらのトランクは、通知先デバイスがNULL_SHA暗号をサポートしていない場合は、そのデバイスを登録したり、コールを発信したりしません。 NULL_SHA 暗号をサポートしていない通知先デバイスでは、**暗号化(Encrypted)** として選択した [デバイスのセキュリティ プロファイル (トランク)] で設定する必要があります。 このデバイス セキュリティ プロファイルを使用すると、トランクは、データの暗号化を可能にする追加の TLS 暗号を提供します。
[着信転送タイプ(Incoming Transport Type)]	[デバイス セキュリティ モード（Device Security Mode）] が [非セキュア（Non Secure）] の場合、TCP+UDP では [転送タイプ（Transport Type）] を指定します。 [デバイスセキュリティモード(Device Security Mode)] が [認証のみ(Authenticated)] または [暗号化(Encrypted)] である場合、[TLS] が転送タイプとなります。 （注） Transport Layer Security（TLS）プロトコルによって、Unified Communications Manager とトランクとの間の接続が保護されます。

設定	説明
[発信転送タイプ(Outgoing Transport Type)]	ドロップダウン リストから適切な発信転送モードを選択します。 [デバイスセキュリティモード(Device Security Mode)] が [非セキュア(Non Secure)] である場合、[TCP] または [UDP] を選択します。 [デバイスセキュリティモード(Device Security Mode)] が [認証のみ(Authenticated)] または [暗号化(Encrypted)] である場合、[TLS] が転送タイプとなります。 （注） TLS は、SIP トランクのシグナリング整合性、デバイス認証、およびシグナリング暗号化を実現します。 （注） Unified Communications Manager システムと、TCP をサポートしていない他のアプリケーションとの間で SIP トランクを接続する場合は、発信トランスポートタイプとして UDP のみを使用する必要があります。 それ以外の場合は、デフォルトオプションとして TCP を使用します。
[ダイジェスト認証を有効化(Enable Digest Authentication)]	ダイジェスト認証を有効にするには、このチェックボックスをオンにします。 このチェックボックスをオンにすると、Unified Communications Manager は、トランクからのすべての SIP 要求でチャレンジを行います。 ダイジェスト認証は、デバイス認証、整合性、および信頼性を提供しません。 これらの機能を使用するには、セキュリティ モード [認証のみ(Authenticated)] または [暗号化(Encrypted)] を選択します。 ヒント TCP 転送または UDP 転送を使用しているトランク上の SIP トランク ユーザを認証するには、ダイジェスト認証を使用してください。
[ナンス確認時間(Nonce Validity Time)]	ナンス値が有効な時間を秒単位で入力します。 デフォルト値は 600（10 分）です。 この時間が経過すると、Unified Communications Manager は新しい値を生成します。 （注） ナンス値は、ダイジェスト認証をサポートするランダム値で、ダイジェスト認証パスワードの MD5 ハッシュの計算に使用されます。

設定	説明
セキュア証明書のサブジェクトまたはサブジェクトの代替名	このフィールドは、[着信転送タイプ(Incoming Transport Type)] および [発信転送タイプ(Outgoing Transport Type)] に TLS を設定した場合に適用されます。 デバイス認証の場合は、SIPトランクデバイスのセキュア証明書のサブジェクトまたはサブジェクト代替名証明書の名前を入力します。Unified Communications Managerクラスタを使用している場合、またはTLSピアにSRVルックアップを使用している場合は、1つのトランクが複数のホストに解決される可能性があり、その結果トランクに複数のセキュア証明書のサブジェクトまたはサブジェクトの代替名が生成されます。 複数のセキュア証明書のサブジェクト名またはサブジェクト代替名が存在する場合は、スペース、カンマ、セミコロン、またはコロンのいずれかの文字を入力して名前を区切ります。 このフィールドには、4096 文字まで入力できます。 **ヒント** サブジェクト名は、送信元接続の TLS 証明書に対応します。 サブジェクト名が、サブジェクト名とポートで一意であることを確認してください。 同じサブジェクト名と着信ポートの組み合わせを異なるSIPトランクに割り当てることはできません。 例：ポート5061のSIP TLS trunk1に、セキュア証明書のサブジェクトまたはサブジェクトの代替名my_cm1、my_cm2があります。 ポート5071のSIP TLS trunk2には、セキュア証明書のサブジェクトまたはサブジェクトの代替名my_cm2、my_cm3があります。 ポート5061のSIP TLS trunk3は、セキュア証明書のサブジェクトまたはサブジェクトの代替名my_ccm4を持つことができますが、セキュア証明書のサブジェクトまたはサブジェクトの代替名my_cm1を持つことはできません。

設定	説明
[着信ポート(Incoming Port)]	着信ポートを選択します。 0 ～ 65535 の一意のポート番号を入力します。 着信 TCP および UDP の SIP メッセージのデフォルトポート値は、5060 です。着信 TLS メッセージの保護されたデフォルト SIP ポートは、5061 です。入力した値は、このプロファイルを使用するすべての SIP トランクに適用されます。 **ヒント** TLS を使用するすべての SIP トランクが、同じ着信ポートを共有できます。[TCP + UDP] を使用するすべての SIP トランクが、同じ着信ポートを共有できます。 同じポートで、TLS の SIP 転送トランクと、TLS 以外の SIP 転送トランク タイプを混合することはできません。 **ヒント** 通常のトラフィック時に、SIP トランクの UDP ポートで 1 つの IP アドレスから着信したパケットのレートが SIP Trunk UDP Port Throttle Threshold の設定値を超えた場合は、しきい値を設定し直します。 SIP トランクと SIP ステーションが同じ着信 UDP ポートを共有している場合、2 つのサービス パラメータ値の大きいほうの値に基づいて Unified Communications Manager はパケットのスロットリングを行います。 このパラメータに対する変更を有効にするには、Cisco CallManager サービスを再起動する必要があります。
[アプリケーションレベル認証を有効化(Enable Application Level Authorization)]	アプリケーションレベルの許可は、SIP トランクを介して接続されるアプリケーションに適用されます。 このチェックボックスをオンにする場合は、**ダイジェスト認証を有効化(Enable Digest Authentication)**チェックボックスもオンにし、トランクのダイジェスト認証を設定する必要があります。Unified Communications Manager は許可されたアプリケーション メソッドを確認する前に SIP アプリケーション ユーザを認証します。 アプリケーション レベルの許可が有効な場合は、まずトランク レベルの許可が発生してから、アプリケーション レベルの許可が発生します。つまり、Unified Communications Manager は、**アプリケーションユーザの設定(Application User Configuration)** ウィンドウで SIP アプリケーションユーザに許可されている方式よりも先に、（このセキュリティ プロファイルで）トランクに許可されている方式を確認します。 **ヒント** アプリケーションの ID を信頼しない場合、またはアプリケーションが特定のトランクで信頼されていない場合は、アプリケーションレベルの許可の使用を検討してください。アプリケーション要求は、予期しないトランクから着信することがあります。

設定	説明
[プレゼンスのSUBSCRIBEの許可（Accept Presence Subscription）]	Unified Communications Manager が SIP トランク経由で着信するプレゼンス サブスクリプション要求を受け付けるようにする場合は、このチェックボックスをオンにします。 **[アプリケーションレベル認証を有効化(Enable Application Level Authorization)]** チェックボックスをオンにした場合は、[アプリケーションユーザの設定(Application User Configuration)]ウィンドウに移動し、この機能について許可するアプリケーション ユーザの **[プレゼンスのSUBSCRIBEの許可(Accept Presence Subscription)]** チェックボックスをオンにします。 アプリケーションレベルの許可が有効で、アプリケーション ユーザの **[プレゼンスのSUBSCRIBEの許可(Accept Presence Subscription)]** チェックボックスがオンで、トランクのチェックボックスがオフの場合、トランクに接続されている SIP ユーザ エージェントに 403 エラー メッセージが送信されます。
[Out-of-Dialog REFERの許可(Accept Out-of-Dialog Refer)]	Unified Communications Manager が SIP トランク経由で着信する非インバイトの Out-of-Dialog REFER 要求を受け付けるようにする場合は、このチェックボックスをオンにします。 [アプリケーションレベル認証を有効化(Enable Application Level Authorization)] チェックボックスをオンにした場合は、[アプリケーションユーザの設定(Application User Configuration)]ウィンドウに移動し、この方式について許可するアプリケーション ユーザの **[Out-of-Dialog REFERの許可(Accept Out-of-Dialog Refer)]** チェックボックスをオンにします。
[Unsolicited NOTIFYの許可(Accept Unsolicited Notification)]	Unified Communications Manager が SIP トランクを経由する受信非インバイト メッセージ、未承諾通知メッセージを受け入れるようにするには、このチェックボックスをオンにします。 **[アプリケーションレベル認証を有効化(Enable Application Level Authorization)]** チェックボックスをオンにした場合は、[アプリケーションユーザの設定(Application User Configuration)]ウィンドウに移動し、この方式について許可するアプリケーションユーザの **[Unsolicited NOTIFYの許可(Accept Unsolicited Notification)]** チェックボックスをオンにします。

設定	説明
[Replacesヘッダーの許可(Accept Replaces Header)]	Unified Communications Manager が既存の SIP ダイアログを置き換える新しい SIP ダイアログを受け付けるようにする場合は、このチェックボックスをオンにします。 **[アプリケーションレベル認証を有効化(Enable Application Level Authorization)]** チェックボックスをオンにした場合は、[アプリケーションユーザの設定(Application User Configuration)]ウィンドウに移動し、この方式について許可するアプリケーション ユーザの **[Replaces ヘッダーの許可(Accept Header Replacement)]** チェックボックスをオンにします。
[セキュリティステータスの送信(Transmit Security Status)]	Unified Communications Manager が、関連付けられた SIP トランクから SIP ピアにコールのセキュリティ アイコン ステータスを送信するようにする場合は、このチェックボックスをオンにします。 デフォルトでは、このチェックボックスはオフになっています。
[SIP V.150アウトバウンドSDPオファーのフィルタリング(SIP V.150 Outbound SDP Offer Filtering)]	ドロップダウン リストから、次のフィルタ処理オプションのいずれかを選択します。 • **[デフォルトのフィルタを使用(Use Default Filter)]**：SIP トランクは、SIP V.150 Outbound SDP Offer Filtering サービス パラメータで示されるデフォルトのフィルタを使用します。サービスパラメータを見つけるには Cisco Unified Communications Manager Administration の**システム（System）** > **サービスパラメータ（Service Parameters）** > **クラスタ全体のパラメータ（デバイス-SIP）（Clusterwide Parameters (Device-SIP)）**に移動します。 • **[フィルタなし(No Filtering)]**：SIP トランクは、アウトバウンド オファーで V.150 SDP 回線のフィルタリングを行いません。 • **[MER V.150 を削除(Remove Pre-MER V.150)]**：SIP トランクは、アウトバウンド オファーで V.150 MER SDP 回線を削除します。トランクが MER V.150 よりも前の Unified Communications Manager に接続する際のあいまいさを低減するには、このオプションを選択します。 • **[MER V.150より前を削除(Remove Pre-MER V.150)]**：SIP トランクは、アウトバウンド オファーで MER に準拠しない V.150 回線があれば削除します。 MER よりも前の回線でオファーを処理できない MER 準拠のデバイスのネットワークに、ご使用のクラスタが含まれているときのあいまいさを低減するには、このオプションを選択します。

設定	説明
[SIP V.150アウトバウンドSDPオファーのフィルタリング(SIP V.150 Outbound SDP Offer Filtering)]	ドロップダウン リストから、次のフィルタ処理オプションのいずれかを選択します。 • **[デフォルトのフィルタを使用(Use Default Filter)]**：SIP トランクは、SIP V.150 Outbound SDP Offer Filtering サービス パラメータで示されるデフォルトのフィルタを使用します。サービスパラメータを見つけるには Cisco Unified Communications Manager Administration の**システム（System）** > **サービスパラメータ（Service Parameters）** > **クラスタ全体のパラメータ（デバイス-SIP）（Clusterwide Parameters (Device-SIP)）**に移動します。 • **[フィルタなし(No Filtering)]**：SIP トランクは、アウトバウンド オファーで V.150 SDP 回線のフィルタリングを行いません。 • **[MER V.150 を削除(Remove Pre-MER V.150)]**：SIP トランクは、アウトバウンド オファーで V.150 MER SDP 回線を削除します。トランクが MER V.150 よりも前の Unified Communications Manager に接続する際のあいまいさを低減するには、このオプションを選択します。 • **[MER V.150より前を削除(Remove Pre-MER V.150)]**：SIP トランクは、アウトバウンド オファーで MER に準拠しない V.150 回線があれば削除します。 MER よりも前の回線でオファーを処理できない MER 準拠のデバイスのネットワークに、ご使用のクラスタが含まれているときのあいまいさを低減するには、このオプションを選択します。 （注） セキュアコール接続を確立するには、V.150用にSIPのIOSを設定する必要があります。 IOS を Unified Communications Manager で設定する際の詳細については、http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.htmlをご覧ください。

SIP トランク セキュリティ プロファイルの適用

トランクの設定 ウィンドウのトランクに SIP トランクセキュリティプロファイルを適用します。 デバイスにセキュリティプロファイルを適用するには、以下の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager アドミニストレーション ガイドの説明に従ってトランクを見つけます。

ステップ 2 **トランク構成** ウィンドウが表示されたら、[**SIP トランクセキュリティプロファイル**] 設定を見つけます。

ステップ 3 **セキュリティプロファイル** ドロップダウンリストから、端末に適用するセキュリティプロファイルを選択します。

ステップ 4 **[保存（Save）]** をクリックします。

ステップ 5 トランクをリセットするには、[**設定の適用**] をクリックします。
SIP トランクのダイジェスト認証を有効にするプロファイルを適用した場合、トランクの **ダイジェスト認証情報** を **SIP レルム** ウィンドウで構成する必要があります。 アプリケーションレベルの認証を有効にするプロファイルを適用した場合、**[アプリケーションユーザー（Application User）]** ウィンドウで、ダイジェスト認証情報と許可される認証方法を設定する必要があります（まだ設定していない場合）。

SIP トランクと SIP トランク セキュリティ プロファイルを同期する

構成が変更された SIP トランクセキュリティプロファイルと SIP トランクを同期するには、以下の手順を実行します。これにより、可能な限り最小の影響で未適用の設定を適用します。(たとえば、影響を受ける一部のデバイスでは、リセット/再起動を実行する必要がない場合があります。)

手順

ステップ 1 **[システム（System）]** > **[セキュリティプロファイル（Security Profile）]** > **[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]** を選択します。

ステップ 2 使用する検索条件を選択します。

ステップ 3 **[検索（Find）]** をクリックします。

ウィンドウには、検索基準に一致する SIP トランクセキュリティプロファイルのリストが表示されます。

ステップ 4 同期するためのSIPトランクセキュリティプロファイルをクリックします。

ステップ 5 追加の設定変更を加えます。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 **[設定の適用（Apply Config）]** をクリックします。

[**設定情報の適用**] ダイアログが表示されます。

ステップ 8 **OK**をクリックします。

Unified Communications Manager Administration を使用して SRTP を許可する

[SRTP 許可] チェックボックスは、 Unified Communications Manager の次の設定ウィンドウに表示されます:

- H.323 ゲートウェイの設定ウィンドウ
- H.225 トランク (ゲートキーパー制御) の設定ウィンドウ
- Inter-Cluster Trunk (ゲートキーパー制御) 設定ウィンドウ
- Inter-Cluster Trunk (ゲートキーパー制御) 設定ウィンドウ
- SIP トランク設定ウィンドウ

H.323 ゲートウェイおよびゲートキーパーまたは非ゲートキーパーで制御される H.323/H.245/H.225 トランクまたは SIP トランクの [SRTP 許可] チェックボックスを設定するには、以下の手順を実行します。

手順

ステップ 1 Unified Communications Manager の説明に従って、ゲートウェイまたはトランクを見つけます。

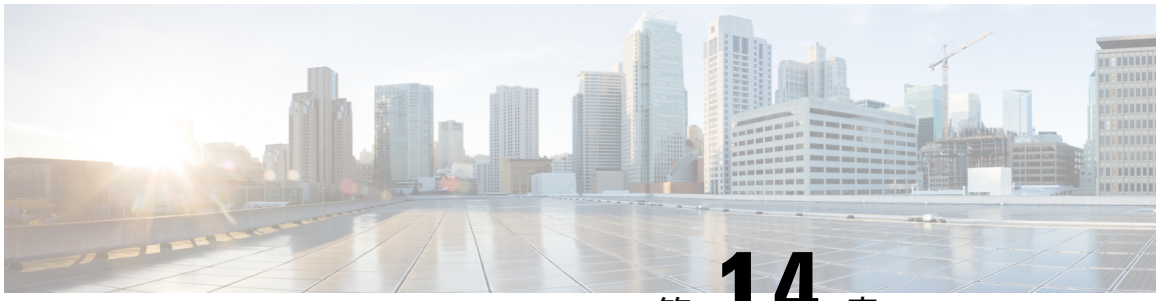
ステップ 2 ゲートウェイ/トランクの設定ウィンドウを開いたら、[**SRTP 許可**]チェックボックスにチェックを入れます。

注意
SIP トランクに対して [**SRTP 許可**] チェックボックスを選択する場合、暗号化された TLS プロファイルを使用することをお勧めします。 安全ではないプロファイルを使用する場合、SRTP は引き続き機能しますが、キーはシグナリングとトレースで公開されます。 この場合、Unified Communications Manager とトランクの接続先の間でネットワークのセキュリティを確保する必要があります。

ステップ 3 **[保存（Save）]** をクリックします。

ステップ 4 端末をリセットするには、 **[リセット] をクリックします**。

ステップ 5 H323 に対して IPSec が正しく構成されていることを確認します。 (SIP の場合、TLS が正しく設定されていることを確認してください。)



第 14 章

Cisco CTL クライアントのセットアップ

この章では、Cisco CTL クライアントのセットアップに関する情報を提供します。

- Cisco CTL セットアップについて （209 ページ）
- 復旧用 CTL ファイルに 2 番目の Sast ロールを追加 （211 ページ）
- CLI による SIP Oauth の構成 （212 ページ）
- Cisco CTL Provider Service をアクティベートする （213 ページ）
- Cisco CAPF サービスのアクティベーション （214 ページ）
- セキュアポートのセットアップ （214 ページ）
- Cisco CTL クライアントのセットアップ （216 ページ）
- SASTのCTLファイルの役割 （218 ページ）
- あるクラスターから別のクラスターに電話を移行する （218 ページ）
- eToken ベースの CTL ファイルからトークンレス CTL ファイルへの移行 （220 ページ）
- CTL ファイルの更新 （220 ページ）
- Cisco Unified Communications Manager セキュリティモードの更新 （221 ページ）
- Cisco CTL ファイルの詳細 （222 ページ）
- Cisco Unified Communications Manager セキュリティモードの確認 （223 ページ）
- Smart Card サービスを開始または自動に設定する （224 ページ）
- Cisco CTL クライアントの確認またはアンインストール （225 ページ）

Cisco CTL セットアップについて

デバイス、ファイル、およびシグナリング認証は、証明書信頼リスト（CTL）ファイルの作成に依存します。このファイルは、Cisco 証明書信頼リスト（CTL）をインストールして設定するときに作成されます。

（注）

- 混合モードを有効にする、または CTL ファイルを更新するには、Unified Communications Manager で、[輸出規制による機能限定の許可（Allow export-controlled functionality）] が有効になっているスマートアカウントまたは仮想アカウントから受け取った登録トークンを使用して、スマートライセンス登録が完了していることを確認します。 Cisco Smart Software Licensing の設定方法については、http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html にある『*Cisco Unified Communications Manager* システム設定ガイド』の「「スマート ソフトウェア ライセンシング」」の章を参照してください。
- CTL クライアントを実行しているときに Unified Communications Manager が輸出規制による機能限定を有効にしていない場合、*ClusterModeSecurityFailedExportControlNotAllow* という名前のアラームが送信されます。

CTL ファイルには、次のサーバまたはセキュリティトークンのエントリが含まれています。

- システム管理者セキュリティトークン（SAST）
- 同一のサーバ上で実行されている CiscoCallManager および CiscoTFTP サービス
- 認証局プロキシ 機能（CAPF）
- TFTP サーバー
- ASA ファイアウォール
- ITL リカバリ

Call Manager 証明書が自己署名の場合、CTL ファイルには各サーバのサーバ証明書、公開キー、シリアル番号、署名、発行者名、サブジェクト名、サーバ機能、DNS 名、および IP アドレスが含まれます。

Multi-SAN Call Manager 証明書の場合、CTL ファイルにはパブリッシャーの Call Manager 証明書が含まれています。

次に電話が初期化されるときに、TFTP サーバから CTL ファイルがダウンロードされます。CTL ファイルに、自己署名証明書を持つ TFTP サーバエントリが含まれている場合、電話機は .sgn 形式の署名付き設定ファイルを要求します。 TFTP サーバに証明書が含まれていない場合、電話機は署名されていないファイルを要求します。

Cisco CTL クライアントがサーバ証明書を CTL ファイルに追加したら、以下の CLI コマンドを実行して CTL ファイルを更新できます。

utils ctl set-cluster 混合モード
CTL ファイルを更新し、クラスタを混合モードに設定します。

utils ctl set-cluster ノンセキュア モード
CTL ファイルを更新し、クラスタをノンセキュア モードに設定します。

utils ctl update CTLFile
クラスターの各ノードで CTL ファイルを更新します。

CTL ファイルにファイアウォールを設定することで、セキュアな Unified Communications Manager システムの一部として Cisco ASA ファイアウォールをセキュアにすることができます。 ファイアウォール証明書が 「CCM」 証明書として表示されます。

（注）
- パブリッシャ ノードで CLI コマンドを実行する必要があります。
- ITLRecovery 証明書を再生成すると、ファイルの署名者が変更されることに注意してください。 Security by Default をサポートしない電話機は、電話機から CTL ファイルを手動で削除しない限り、新しい CTL ファイルを受け入れません。 電話からの CTL ファイルの削除については、お使いの電話モデルの *Cisco IP Phone* 管理ガイド を参照してください。

復旧用 CTL ファイルに 2 番目の Sast ロールを追加

Unified Communications Manager の以前のリリースでは、エンドポイントが 1 つの Cisco サイト管理者セキュリティトークン（SAST）のみを信頼するトークンレスのアプローチがありました。 この SAST（セキュリティ認証サービストークン）は、CallManager 証明書です。 このアプローチでは、証明書信頼リスト（CTL）ファイルには、CTL ファイルの署名に使用される 1 つの SAST（セキュリティ認証サービストークン）レコードのみが含まれていました。 1 つの SAST（セキュリティ認証サービストークン）のみが使用されたため、SAST（セキュリティ認証サービストークン）署名者を更新すると、エンドポイントがロックアウトされました。 以下のポイントは、SAST（セキュリティ認証サービストークン）署名者の更新が原因でエンドポイントまたはデバイスがロックアウトされたシナリオを示しています。

- エンドポイントは、登録時に CallManager 証明書を使用して署名された CTL ファイルを受け入れました。
- 管理者が CallManager 証明書を再生成し、CTL ファイルを更新しました。 この再生成は、更新された CTL ファイルが既存の CallManager 証明書ではなく、更新された CallManager 証明書によって署名されていることを意味していました。
- エンドポイントは更新された CallManager 証明書を信頼しませんでした。エンドポイントの信頼リストに更新された証明書がなかったからです。そのため、エンドポイントは CTL ファイルをダウンロードせずに拒否しました。
- エンドポイントが、Transport Layer Security (TLS) 経由で安全に ccm サービスに接続しようとしました。ccmservice は、TLS 交換の一部としてエンドポイントに更新された CallManager 証明書を提供しました。 更新された証明書がエンドポイントの信頼リストになかったため、エンドポイントが CTL ファイルをダウンロードせずに拒否しました。
- エンドポイントは ccmservice と通信せず、結果としてロックアウトされます。

エンドポイントのロックアウトからのリカバリを容易にするために、エンドポイントのトークンレスアプローチは、リカバリ用の CTL ファイルに 2 番目の Sast を追加することで強化され

ています。この機能では、トークンレスCTLファイルには、CallManagerレコードとITLRecoveryレコードの 2 つの Sast トークンが含まれます。

ITLRecovery 証明書は、以下の理由により、他の証明書よりも選択されます。

- ホスト名の変更など、二次的な理由により変更されません。
- ITL ファイルですでに使用されています。

CLI による SIP Oauth の構成

CLI を通じて、クラスター SIP Oauth モードを設定できます。

（注） Cisco Unified Communications Manager で SIP OAuth モードを設定する方法の詳細は、『*Cisco Unified Communications Manager* 機能設定ガイド、リリース *12.5(1)*』を参照してください。

以下の点を考慮してください。

- クラスターSIP OAuthモードが有効な場合、Cisco Unified Communications Managerはセキュアなデバイスからの OAuth トークンによる SIP 登録を受け付けます。

  有効にすると、次の TLS ポートが開きます。これらはCisco Unified Communications Managerユーザインターフェイスから設定できます。

  - **SIP Oauth ポート**
  - **SIP Oauth MRA ポート**

  Cisco Unified CM Administration でポートを設定できます。**[システム（System）]** > **[Cisco Unified CM]** > **[CallManager]** ページを選択します。

- パラメータの変更を有効にするために、すべてのノードでCisco CallManagerサービスを再起動します。

暗号化オプションは以下の CLI コマンドで構成されています。

admin:utils sipOAuth-mode
クラスターの SIP OAuth モードの状況を確認します。
utils sipOAuth-mode enable
クラスターで SIP Oauth モードを有効にします。
utils sipOAuth-mode disable
クラスターで SIP Oauth モードを無効にします。

（注） パブリッシャノードでのみ CLI コマンドを実行します。

Cisco CTL Provider Service をアクティベートする

Cisco CTL クライアントを設定すると、Cisco CTL プロバイダサービスによりセキュリティモードがノンセキュアから混合モードに変更され、サーバー証明書が CTL ファイルに転送されます。 その後、サービスは CTL ファイルをすべての Unified Communications Manager および CiscoTFTP サーバーに転送します。

このサービスを有効にしてから Unified Communications Manager をアップグレードすると、Unified Communications Manager はアップグレード後に自動的にサービスを再有効化します。

ヒント クラスタ内のすべてのサーバーで CiscoCTL プロバイダサービスを有効にする必要があります。

サービスを有効にするには、次の手順を実行します。

手順

ステップ 1 Cisco Unified Serviceability で、**[ツール（Tools）] > [サービスのアクティブ化（Service Activation）]** の順に選択します。

ステップ 2 [サーバ] ドロップダウン リスト ボックスで、Cisco CallManager または Cisco TFTP サービスを有効にしたサーバを選択します。

ステップ 3 [**CiscoCTL プロバイダ**] サービスのラジオボタンをクリックします。

ステップ 4 [保存（Save）]をクリックします。

ヒント
クラスタ内のすべてのサーバでこの手順を実行します。

（注）
CiscoCTL Provider サービスを有効にする前に、CTL ポートを入力することができます。 デフォルトのポート番号を変更する場合は、TLS 接続用のポートの設定に関するトピックを参照してください。

ステップ 5 サーバー上でサービスが実行されていることを確認します。 Cisco Unified Serviceability で **[ツール（Tools）] > [コントロールセンター - 機能サービス（Control Center - Feature Services）]** を選択し、サービスの状態を確認します。

Cisco CAPF サービスのアクティベーション

警告 Cisco CTL クライアントをインストールして設定する前に Cisco 認証局プロキシ機能サービスをアクティブ化することで、CAPF を使用するために CTL ファイルを更新する必要がなくなります。

セキュアポートのセットアップ

デフォルトのポートが現在使用されている場合、またはファイアウォールを使用しており、ファイアウォール内のポートを使用できない場合は、別の TLS ポート番号を設定する必要があります。

- TLS 接続のための Cisco CTL プロバイダのデフォルトポートは 2444 です。Cisco CTL Provider ポートは Cisco CTL クライアントからのリクエストを監視します。 このポートは、CTL ファイルの取得、クラスタセキュリティモードの設定、TFTP サーバへの CTL ファイルの保存など、Cisco CTL クライアントの要求を処理します。

（注） クラスタセキュリティモードでは、スタンドアロンサーバまたはクラスタのセキュリティ機能を設定します。

- イーサネット電話ポートは、SCCP を実行している電話からの登録要求を監視します。 非セキュアモードでは、電話はポート 2000 を通して接続します。混合モードでは、TLS 接続用の Unified Communications Manager ポートは、Unified Communications Manager ポート番号に443を加えた値となります。このため、Unified Communications Manager のデフォルトの TLS 接続は 2443 となります。ポート番号が使用中であるか、ファイアウォールを使用していてその中でポートを使用できない場合にのみ、この設定を更新します。
- SIP セキュアポートにより、 Unified Communications Manager は、SIP を実行している電話からの SIP メッセージをリッスンすることができます。 デフォルト値は 5061 です。このポートを変更する場合、Cisco Unified Serviceability で Cisco CallManager サービスを再起動し、SIP を実行している電話機をリセットする必要があります。

ヒント ポートを更新したら、Cisco Unified Serviceability で Cisco CTL Provider サービスを再起動する必要があります。

ヒント　CTL クライアントが実行されているデータ VLAN に対して CTL ポートを開く必要があります。

デフォルト設定を変更するには、以下の手順を実行します。

手順

ステップ 1　変更するポートに応じて、以下のタスクを実行します。

a) Cisco CTL Provider サービスのポート番号パラメータを変更するには、ステップ 2 （215 ページ） から ステップ 6 （215 ページ） までの手順を実行します。

b) イーサネット電話ポートまたは SIP 電話セキュアポートの設定を変更するには、ステップ 7 （215 ページ） から ステップ 11 （215 ページ）を実行します。

ステップ 2　Cisco CTL プロバイダポートを変更するには、Unified Communications Manager Administration で **[システム（System）]** > **[サービスパラメータ（Service Parameters）]** を選択します。

ステップ 3　[サーバ] ドロップダウンリストで、CiscoCTL プロバイダー サービスが実行されるサーバを選択します。

ステップ 4　[サービス] ドロップダウンリストボックスから、 Cisco CTL Provider サービスを選択します。

ヒント
サービスパラメータの詳細については、疑問符またはリンク名をクリックしてください。

ステップ 5　ポート番号パラメータの値を変更するには、[パラメータ値]フィールドに新しいポート番号を入力します。

（注）
12.X 以降、[パラメータ値] フィールドで [ポート番号] パラメータの値を変更することはできません。

ステップ 6　[保存（Save）]をクリックします。

ステップ 7　イーサネット電話ポートまたは SIP 電話セキュアポートの設定を変更するには、Unified Communications Manager Administration で **[システム（System）]** > **[CiscoUnifiedCM]** を選択します。

ステップ 8　『 *Cisco Unified Communications Manager* 管理ガイド』の説明に従って、CiscoCallManager サービスが実行されているサーバを検索します。結果が表示されたら、サーバの **名前** リンクをクリックします。

ステップ 9　Unified Communications Manager 設定ウィンドウが表示されたら、[イーサネット電話ポート] または [SIP 電話セキュアポート] フィールドに新しいポート番号を入力します。

ステップ 10　電話をリセットし、Cisco Unified Serviceability で CiscoCallManager サービスを再起動します。

ステップ 11　**[保存（Save）]** をクリックします。

Cisco CTL クライアントのセットアップ

重要 **utils ctl** CLI コマンドセットを使用して、暗号化をセットアップできます。 CLI の使用の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

（注）
- CLI コマンド **utils ctl set-cluster mixed-mode** は、クラスタを混合モードに設定します。 混合モードを有効にするには、Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されていること、およびスマートアカウントまたはバーチャルアカウントから受信した登録トークンで [輸出規制による機能限定の許可（Allow export-controlled functionality）] が有効になっており、そのトークンがこのクラスタに登録されていることを確認します。
- CLI コマンド **utils ctl update CTLFile** は、CTLFile を更新します。 CTLFIle を混合モードで更新するには、Unified Communications Manager が Cisco Smart Software Manager または Cisco Smart Software Manager サテライトに登録されていること、およびスマートアカウントまたはバーチャルアカウントから受信した登録トークンで [輸出規制による機能限定の許可（Allow export-controlled functionality）] が有効になっており、そのトークンがこのクラスタに登録されていることを確認します。
- Unified Communications Manager が、[輸出規制による機能限定の許可（Allow export-controlled functionality）] が有効になっている登録トークンで登録されておらず、さらに **utils ctl set-cluster mixed-mode** および **utils ctl update CTLFile** コマンドを実行すると、次のエラーメッセージが表示されます。

  `Unified Communications Manager クラスタが ［輸出規制による機能限定の許可（Allow export-controlled functionality）］ でスマート/仮想アカウントに登録されていないため、コマンドを実行できません。 UCM クラスターの登録時に、スマート/仮想アカウントから受け取った製品トークンで ［輸出規制による機能限定の許可（Allow export-controlled functionality）］ にチェックが入っていることを確認します。`

Cisco CTL CLI は以下のタスクを実行します。

- クラスタサーバまたはスタンドアロンサーバの Unified Communications Manager セキュリティモードを設定します。

（注） Unified Communications Manager クラスタ セキュリティ パラメータを、Unified Communications Manager Administration の [エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ウィンドウから混合モードに設定することはできません。 クラスタセキュリティモードは、Cisco CTL クライアントまたは CLI コマンド set **utils ctl** で設定できます。

- 証明書信頼リスト（CTL）を作成します。これは、セキュリティトークン、Unified Communications Manager、ASA ファイアウォール、CAPF サーバーの証明書エントリを含むファイルです。

  CTL ファイルは、電話接続の TLS をサポートするサーバを示します。 クライアントは、Unified Communications Manager、Cisco CAPF、および ASA ファイアウォールを自動的に検出し、これらのサーバーの証明書エントリを追加します。

（注） Cisco CTL クライアントは、スーパークラスタサポートも提供：最大 16 台のコール処理サーバー、1 台のパブリッシャ、2 台の TFTP サーバー、そして最大 9 台のメディアリソースサーバーをサポートします。

ヒント TFTP サービスを再起動してから、クラスタ内でこれらのサービスを実行するすべてのサーバー上で CallManager を再起動する必要があるため、スケジュールされたメンテナンス期間中に CTL ファイルを更新できます。

Cisco CTL の設定が完了した後、CTL は以下のタスクを実行します。

- CTL ファイルを Unified Communications Manager サーバー（複数可）に書き込みます。
- CAPF capf.cer をクラスタ内のすべての Unified Communications Manager 後続ノード(最初のノードではない)に書き込みます。
- クラスタ内のすべての Unified Communications Manager の後続ノード (最初のノードではない) に PEM 形式の CAPF 証明書ファイルを書き込みます。
- すべての設定済み TFTP サーバにファイルを書き込みます。
- 設定済みのすべての ASA ファイアウォールにファイルを書き込みます。
- CTL ファイルの作成時に USB ポート内に存在していたセキュリティトークンの秘密鍵を使って、CTL ファイルに署名します。

SASTのCTLファイルの役割

（注） *次の表に記載されている署名者は、CTL ファイルへの署名に使用されます。

表 *31 :* システム管理者セキュリティトークン（*SAST*）の*CTL*ファイルの役割

Cisco Unified Communications Manager のバージョン	トークンベースのCTLファイルのシステム管理者セキュリティトークン（SAST）の役割	トークンレスのCTLファイルのシステム管理者セキュリティトークン（SAST）の役割
12.0(1)	トークン 1 (署名者*) トークン 2 ITL リカバリ CallManager	ITLRecovery (署名者) CallManager
11.5(x)	トークン 1 (署名者) トークン 2 ITL リカバリ CallManager	CallManager (署名者) ITL リカバリ
10.5(2)	トークン 1 (署名者) トークン 2	CallManager (署名者) ITL リカバリ
10.5(1) (サポートされていません)	トークン 1 (署名者) トークン 2	CallManager (署名者)
10.0(1) (サポートされていません)	トークン 1 (署名者) トークン 2	CallManager (署名者)
9.1(2)	トークン 1 (署名者) トークン 2	なし

あるクラスターから別のクラスターに電話を移行する

次の手順を使用して、電話を1つのクラスタから別のクラスタに移行します。たとえば、クラスター 1 からクラスター 2 に。

手順

ステップ 1 Cisco Unified OS Administration のクラスタ 2 から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

ステップ 2 **[検索（Find）]** をクリックします。

ステップ 3 証明書のリストから、ITLRecovery 証明書をクリックし、**[.PEM ファイルのダウンロード（Download .PEM File）]** または **[.DER ファイルのダウンロード（Download .DER File）]** のいずれかをクリックして、いずれかのファイル形式の証明書をコンピュータにダウンロードします。
証明書の詳細が表示されます。

ステップ 4 証明書のリストから、CallManager 証明書をクリックし、**[.PEM ファイルのダウンロード（Download .PEM File）]** または **[.DER ファイルのダウンロード（Download .DER File）]** のいずれかをクリックして、いずれかのファイル形式の証明書をコンピュータにダウンロードします。
証明書の詳細が表示されます。

ステップ 5 Cisco Unified OS Administration のクラスタ 1 から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。
[証明書の一覧（Certificate List）]ウィンドウが表示されます。

ステップ 6 **証明書チェーンのアップロード**をクリックして、ダウンロードした証明書をアップロードします。

ステップ 7 [証明書の目的（Certificate Purpose）] ドロップダウンリストで、[Phone-SAST-trust] を選択します。

ステップ 8 **[ファイルのアップロード（Upload File）]** フィールドについて、**[ファイルを選択（Choose File）]** をクリックし、ステップ 3 でダウンロードした ITLRecovery ファイルを参照し、**[ファイルをアップロード（Upload File）]** をクリックします。
アップロードされた ITLRecovery ファイルは、クラスタ 1 の **[証明書一覧（Certificate List）]** ウィンドウに **Phone-SAST-Trust** 証明書として表示されます。新しい ITL ファイルにクラスタ 2 の ITLRecovery 証明書がある場合は、コマンド `show itl` を実行します。

ステップ 9 クラスタ 1 の電話にローカルで有効な証明書 (LSC) がある場合、クラスタ 1 からの CAPF 証明書はクラスタ 2 の CAPF 信頼ストアにアップロードされる必要があります。

ステップ 10 （任意） この手順は、クラスターが混合モードの場合にのみ適用できます。 CLI で **utils ctl update CTLFile** コマンドを実行し、クラスター 1 で CTL ファイルを再生成します。

（注）
- `show ctl` CLI コマンドを実行して、クラスタ 2 の ITLRecovery 証明書と CallManager 証明書が、SASTの役割を持つ CTL ファイルに含まれていることを確認します。
- 電話が新しい CTL および ITL ファイルを受信したことを確認します。 更新された CTL ファイルには、クラスター 2 の ITLRecovery 証明書があります。

クラスタ 1 からクラスタ 2 に移行する電話は、クラスタ 2 の ITLRecovery 証明書を受け入れるようになります。

ステップ 11　1 つのクラスタから別のクラスタに電話を移行します。

eToken ベースの CTL ファイルからトークンレス CTL ファイルへの移行

トークンレス CTL ファイルの場合、管理者は、Unified Communications Manager リリース 12.0(1) 以降で、USB トークンを使用して生成され、アップロードされた CTL ファイルをエンドポイントがダウンロードするようにする必要があります。 ダウンロード後、トークンレス CTL ファイルに切り替えることができます。 その後、 `util ctl update` CLI コマンドを実行できます。

CTL ファイルの更新

（注）　CLI コマンドの set **utils ctl でクラスターのセキュリティを管理する場合、この手順は必要ありません。**

次のシナリオが発生した場合、CTL ファイルを更新する必要があります。 以下を行った場合：

- 新しい Unified Communications Manager サーバーをクラスタに追加した場合

（注）　セキュアなクラスタにノードを追加するには、「*Unified Communications Manager* をインストールする」を参照してください。新しいノードの追加方法と新しいノードのセキュリティ設定方法について説明しています。

- Unified Communications Manager サーバーの名前または IP アドレスを変更した場合
- 設定済みの TFTP サーバーの IP アドレスまたはホスト名を変更した場合
- 設定済みの ASA ファイアウォールの IP アドレスまたはホスト名を変更した場合
- Cisco 認証局機能サービスを Cisco Unified Serviceability で有効にした場合
- セキュリティトークンを追加または削除した場合
- TFTP サーバーを追加または削除した場合
- Unified Communications Manager サーバーを追加または削除した場合
- ASA ファイアウォールを追加または削除した場合

- CTL ファイルを含む Cisco Unified Communications Manager クラスタ上の任意のノードで、CallManager、CAPF、または ITL 回復証明書を手動で再生成する場合は、CTL ウィザードを再実行する必要があります。 この手順は、他の証明書の生成には必要ありません。
- 7.1.5 以前の Unified Communications Manager バージョンを 7.1.5 またはそれ以降のバージョンに更新した場合。
- 10.5 より前の Unified Communications Manager バージョンを 10.5 以降に更新した場合は、「ハードウェア eToken からトークンレス ソリューションへの移行」の項を参照してください。
- サードパーティの CA 署名付き証明書をプラットフォームにアップロードした場合。

（注） 混合モードの Unified Communications Manager クラスタでドメイン名が追加または変更された場合、電話構成ファイルを有効にするために CTL ファイルを更新する必要があります。

ヒント 最小限のコール処理の中断が発生するときにファイルを更新することを強くお勧めします。

注意 Unified Communications Manager が安全な SIP または SCCP を使用して Unity Connection 10.5 以降と統合されている場合、セキュアコールが Unity Connection で機能しなくなる場合があります。 この問題を解決するには、Unity Connection の対応するポート グループをリセットする必要があります。

Unity Connection Administration インターフェイスからポートグループをリセットするには、リセットするポートグループを選択し、**[ポートグループの基本（Port Group Basics）]** ページで **[リセット（Reset）]** をクリックした後、**[テレフォニー統合（Telephony Integrations）]** > **[ポートグループ（Port Group）]** に移動します。

Cisco Unified Communications Manager セキュリティモードの更新

クラスタ セキュリティ モードを設定するには、Cisco CTL を使用する必要があります。 Unified Communications Manager Administration の [エンタープライズパラメータの設定（Enterprise Parameters Configuration）] ウィンドウから Unified Communications Manager セキュリティモードを変更することはできません。

（注） クラスタセキュリティモードは、スタンドアロンサーバまたはクラスタのセキュリティ機能を設定します。

Cisco CTL クライアントの初期設定後にクラスタ セキュリティ モードを変更するには、CTL ファイルを更新する必要があります。

手順

ステップ 1 CLI コマンド `utils ctl set-cluster mixed-mode` を実行して、クラスタセキュリティモードをセキュアに変更します。

ステップ 2 CLI コマンド `utils ctl set-cluster non-secure-mode` を実行して、クラスタセキュリティモードを非セキュアに変更します。

Cisco CTL ファイルの詳細

（注） **utils ctl** CLI コマンドセットを使用して暗号化をセットアップできます。これにはセキュリティトークンは必要ありません。 CLI の使用の詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

クラスタ セキュリティ モードは、次の表に示すように、非セキュア モードまたは混合モードに設定できます。 混在モードのみが、認証、暗号化シグナリング、暗号化メディアをサポートしています。

（注） クラスタセキュリティモードは、スタンドアロンサーバまたはクラスタのセキュリティ機能を設定します。

表 *32 : CTL* の設定項目

設定	説明
Unified Communications Manager サーバ	
Security Mode	
Unified Communications Manager クラスタを混合モードに設定する	混合モードでは、認証済み、暗号化済み、ノンセキュア Cisc 録が許可されます。 このモードでは、 Unified Communication セキュアなポートを使用することを保証します。

設定	説明
Unified Communications Manager クラスタを非セキュアモードに設定する	非セキュアモードに設定すると、すべてのデバイスが未認は画像認証のみに対応します。 このモードを選択すると、Cisco CTL クライアントは、CT証明書を削除しますが、CTL ファイルは指定したディレク定ファイルをリクエストし、Unified Communications Mana **ヒント** 電話をデフォルトのノンセキュアモードに戻すには、電話から CTL ファイルを削除する必要があります。
CTL エントリ	
トークン	サーバまたはワークステーションに最初に挿入したトーケーションから次のトークンを挿入するように指示されたす。 追加トークンのセキュリティトークン情報が表示さリティ トークンについて、これらのタスクを繰り返しま
TFTP サーバの追加	証明書信頼リストに代替 TFTP サーバを追加するには、こは、[代替 TFTP サーバー（Alternate TFTP Server）] タブのクリックします。 設定を入力したら、[**次へ**] をクリック
ファイアウォールの追加	このボタンをクリックして、証明書信頼リストに ASA フは、[ファイアウォール（Firewall）] タブの設定が表示さいます。 設定を入力したら、[**次へ**] をクリックします。

Cisco Unified Communications Manager セキュリティモードの確認

クラスタセキュリティモードを確認するには、以下の手順を実行します。

（注） クラスタセキュリティモードは、スタンドアロンサーバまたはクラスタのセキュリティ機能を設定します。

手順

ステップ 1 Unified Communications Manager の管理で、 **[システム]** > **[エンタープライズパラメータの設定]** を選択します。

ステップ 2 **クラスターセキュリティモード** フィールドを見つけます。 フィールドの値が **1** と表示される場合、 Unified Communications Manager が混在モードで正しく設定されています。 (フィールド名をクリックすると詳細が表示されます。)

ヒント
この値は Unified Communications Manager Administration では設定できません。 この値は、Cisco CTL クライアントを設定した後に表示されます。

Smart Card サービスを開始または自動に設定する

Cisco CTL クライアントのインストールにより、Smart Card サービスが無効になっていることが検出された場合、Cisco CTL クライアントプラグインをインストールするサーバーまたはワークステーションで、Smart Card サービスを自動および開始に設定する必要があります。

ヒント サービスが開始済みおよび自動に設定されていない場合、CTL ファイルにセキュリティトークンを追加できません。

ヒント オペレーティングシステムのアップグレード、サービスリリースの適用、Cisco Unified Communications Manager のアップグレードなどの処理を行った後は、Smart Card サービスが自動的に開始されることを確認します。

サービスを開始および自動に設定するには、以下の手順を実行します。

手順

ステップ 1 Cisco CTL クライアントをインストールしたサーバーまたはワークステーションで、**[スタート（Start）] > [プログラム（Programs）] > [管理ツール（Administrative Tools）] > [サービス（Services）]** を選択します。または **[スタート（Start）] > [コントロールパネル（Control Panel）] > [管理ツール（Administrative Tools）] > [サービス（Services）]** を選択します。

ステップ 2 [サービス] ウィンドウから [**Smart Card**] サービスを右クリックし、[プロパティ] を選択します。

ステップ 3 [プロパティ（Properties）] ウィンドウで、**[全般（General）]** タブが表示されることを確認します。

ステップ 4 [スタートアップの種類（Startup type）] ドロップダウンリストから、**[自動（Automatic）]** を選択します。

ステップ 5 [適用（Apply）]をクリックします。

ステップ 6 [サービス状況（Service Status）] エリアで、**[開始（Start）]** をクリックします。

ステップ 7 **OK**をクリックします。

ステップ 8 サーバまたはワークステーションを再起動し、サービスが実行中であることを確認します。

Cisco CTL クライアントの確認またはアンインストール

Cisco CTL クライアントをアンインストールしても、CTL ファイルは削除されません。 同様に、クライアントをアンインストールしても、クラスタ セキュリティ モードと CTL ファイルは変更されません。 そうしたい場合は、CLI オプションを使用して Cisco CTL をアンインストールできます。

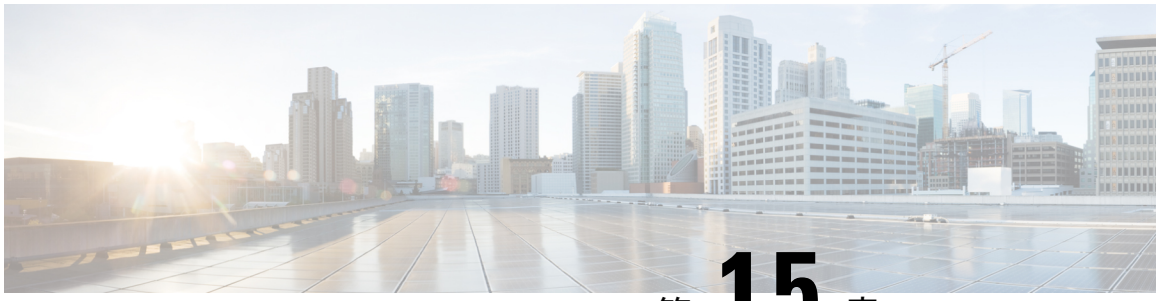
Cisco CTL クライアントがインストールされていることを確認するには、以下の手順を実行します。

手順

ステップ 1 **[スタート（Start）]>[コントロールパネル（Control Panel）]>[プログラムの追加と削除（Add Remove Programs）]** を選択します。

ステップ 2 クライアントがインストールされたことを確認するには、 **Cisco CTL Client** を探します。

ステップ 3 クライアントをアンインストールするには、[**削除**] をクリックします。



第 15 章

TLS セットアップ

- TLS の概要 （227 ページ）
- TLS 前提条件 （227 ページ）
- TLS 設定タスク フロー （228 ページ）
- TLS の連携動作および制限 （234 ページ）

TLS の概要

Transport Layer Security（TLS）はセキュアポートと証明書交換を使用して、2 つのシステム間またはデバイス間でセキュアで信頼できるシグナリングやデータ転送を実現します。 TLS は、Unified Communications Manager が制御するシステム、デバイス、プロセス間の接続を保護および制御し、音声ドメインへのアクセスを防止します。

TLS 前提条件

最低 TLS バージョンを設定する前に、ネットワーク デバイスとアプリケーションの両方でその TLS バージョンがサポートされていることを確認します。 また、それらが、Unified Communications Manager と IM and Presence Services で設定する TLS で有効になっていることを確認します。 次の製品のいずれかが展開されているなら、最低限の TLS 要件を満たしていることを確認します。 この要件を満たしていない場合は、それらの製品をアップグレードします。

- Skinny Client Control Protocol（SCCP）Conference Bridge
- トランスコーダ（Transcoder）
- ハードウェア メディア ターミネーション ポイント（MTP）
- SIP ゲートウェイ
- Cisco Prime Collaboration Assurance
- Cisco Prime Collaboration Provisioning
- Cisco Prime Collaboration Deployment

- Cisco Unified Border Element（CUBE）
- Cisco Expressway
- Cisco TelePresence Conductor

会議ブリッジ、メディアの終了点（MTP）、Xcoder、Prime Collaboration Assurance、Prime Collaboration Provisioning、Cisco Unity Connection、Cisco Meeting Server、Cisco IP 電話、Cisco Room Devices、Fusion Onboarding Service（FOS）などのクラウドサービス、Common Identity Service、Smart License Manager（SLM）、プッシュ REST サービス、Cisco Jabber および Webex アプリクライアントと他のサードパーティアプリケーションをアップグレードすることはできません。

（注） Unified Communications Manager の旧リリースからアップグレードする場合は、上位のバージョンの TLS を設定する前に、すべてのデバイスとアプリケーションでそのバージョンがサポートされていることを確認します。 例えば、Unified Communications Manager と IM and Presence Services のリリース 9.x でサポートされるのは、TLS 1.0 のみです。

TLS 設定タスク フロー

以下のタスクを完了して、TLS 接続用に Unified Communications Manager を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	最小 TLS バージョンの設定 （229 ページ）.	デフォルトでは、Unified Communications Manager において、最小 TLS バージョンとして 1.0 がサポートされています。セキュリティがより高いバージョンの TLS を必要とする場合、システムは TLS 1.1 または 1.2 を使用するように再設定する必要があります。
ステップ 2	（任意） TLS 暗号化の設定 （230 ページ）.	Unified Communications Manager がサポートする TLS 暗号オプションを設定します。
ステップ 3	SIP トランク セキュリティ プロファイルでの TLS の設定 （230 ページ）.	TLS 接続を SIP トランクに割り当てます。 このプロファイルを使用するトランクは、シグナリングに TLS を使用します。セキュアなトランクを使用して、会議ブリッジなどのデバイスに TLS 接続を追加することもできます。

	コマンドまたはアクション	目的
ステップ 4	SIP トランクへのセキュア プロファイルの追加 （231 ページ）.	TLS が有効な SIP トランク セキュリティ プロファイルを SIP トランクに割り当て、トランクが TLS をサポートできるようにします。 セキュアなトランクを使用して、電話会議ブリッジなどのリソースに接続できます。
ステップ 5	電話セキュリティ プロファイルでの TLS の設定 （231 ページ）.	TLS 接続を電話セキュリティ プロファイルに割り当てます。 このプロファイルを使用する電話は、シグナリングに TLS を使用します。
ステップ 6	セキュアフォンプロファイルを電話に追加する （232 ページ）.	作成した TLS が有効なプロファイルを電話に割り当てます。
ステップ 7	セキュア電話プロファイルをユニバーサル デバイス テンプレートに追加する （233 ページ）.	TLS が有効な電話セキュリティ プロファイルをユニバーサル デバイス テンプレートに割り当てます。 このテンプレートで LDAP ディレクトリ同期を設定すると、LDAP 同期で電話にセキュリティをプロビジョニングできます。

最小 TLS バージョンの設定

デフォルトでは、Unified Communications Manager において、最小 TLS バージョンとして 1.0 がサポートされています。 Unified Communications Manager および IM and Presence Service の最低サポート TLS バージョンを 1.1 または 1.2 などの上位バージョンにリセットするには、次の手順を使用します。

設定対象の TLS バージョンが、ネットワーク内のデバイスとアプリケーションでサポートされていることを確認します。 詳細については、TLS 前提条件 （227 ページ）を参照してください。

手順

ステップ 1 **コマンドライン インターフェイス**にログインします。

ステップ 2 既存の TLS のバージョンを確認するには、**show tls min-version** CLI コマンドを実行します。

ステップ 3 **set tls min-version**<*minimum*> CLI コマンドを実行します。ここで、<*minimum*> は TLS のバージョンを示します。

たとえば、最低 TLS バージョンを 1.2 に設定するには、**set tls min-version 1.2** を実行します。

（注）

リリース 15SU1 までは、すべての Unified Communications Manager および IM and Presence Service のサービスクラスタノードで、**ステップ 3** を実行します。

TLS 暗号化の設定

SIP インターフェイスの使用可能な最も強力な暗号化を選択することによって、弱い暗号化を無効にできます。 TLS 接続を確立するために Unified Communications Manager でサポートされる暗号化を設定するには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 [セキュリティ パラメータ（Security Parameters）]で、[TLS 暗号化（TLS Ciphers）]エンタープライズパラメータの値を設定します。 使用可能なオプションについては、エンタープライズパラメータのオンラインヘルプを参照してください。

ステップ 3 **[保存]** をクリックします。

（注）
すべての TLS 暗号は、クライアント暗号の設定に基づいてネゴシエートされます。

SIP トランク セキュリティ プロファイルでの TLS の設定

この手順を使用して、TLS接続をSIPトランクセキュリティプロファイルに指定します。 このプロファイルを使用するトランクは、シグナリングに TLS を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[セキュリティ（Security）]** > **[SIP トランクのセキュリティプロファイル（SIP Trunk Security Profile）]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして、新しい電話セキュリティ プロファイルを作成します。
- **[検索（Find）]** をクリックして検索し、既存のテンプレートを選択します。

ステップ 3 [**名前**] フィールドにプロファイルの名前を入力します。

ステップ 4 **端末セキュリティモード** フィールドの値を **暗号化** または **認証済み**に設定します.

ステップ 5 **[着信トランスポートタイプ（Incoming Transport Type）]** と **[発信トランスポートタイプ（Outgoing Transport Type）]** の両方のフィールド値を **[TLS]** に設定します。

ステップ 6 [**SIP トランクセキュリティプロファイル**] ウィンドウの残りのフィールドに入力します。フィールドとその設定のヘルプについては、オンラインヘルプを参照してください。

ステップ 7 **[保存（Save）]** をクリックします。

SIP トランクへのセキュア プロファイルの追加

この手順を使用して、TLS が有効な SIP トランクセキュリティプロファイルを SIP トランクに指定します。 このトランクを使用して、会議ブリッジなどのリソースへの安全な接続を作成できます。

手順

ステップ 1 Cisco Unified CM Administration から、**[デバイス（Device）]** > **[トランク（Trunk）]** を選択します。

ステップ 2 **[検索（Find）]** をクリックして検索し、既存のテンプレートを選択します。

ステップ 3 [**端末名**] フィールドにトランクの端末名を入力します。

ステップ 4 [**端末プール**] ドロップダウンリストから端末プールを選択します。

ステップ 5 [**SIP プロファイル**] ドロップダウンリストから、SIP プロファイルを選択します。

ステップ 6 [**SIP トランクセキュリティプロファイル**] ドロップダウンリストから、前のタスクで作成した TLS 対応の SIP トランクプロファイルを選択します。

ステップ 7 **宛先** エリアに宛先 IP アドレスを入力します。 最大 16 件の宛先アドレスを入力できます。 追加の宛先を入力するには、[+] ボタンをクリックします。

ステップ 8 **トランク設定**ウィンドウの残りのフィールドをすべて入力します。フィールドとその設定に関するヘルプは、オンラインヘルプを参照してください。

ステップ 9 **[保存（Save）]** をクリックします。

（注）
トランクをセキュア デバイスに接続している場合、セキュア デバイスの証明書を Unified Communications Manager にアップロードする必要があります。 証明書の詳細については、 **証明書** のセクションを参照してください。

電話セキュリティ プロファイルでの TLS の設定

この手順を使用して、TLS接続を電話セキュリティ プロファイルに指定します。 このプロファイルを使用する電話は、シグナリングに TLS を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）]** > **[セキュリティ（Security）]** > **[電話セキュリティプロファイル（Phone Security Profile）]** の順に選択します。

ステップ 2 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[新規追加（Add New）]をクリックします。
- **[検索（Find）]** をクリックして検索し、既存のテンプレートを選択します。

ステップ 3 新しいプロファイルを作成する場合は、電話のモデルとプロトコルを選択し、**[次へ]をクリックします。**

（注）
ユニバーサル端末テンプレートと LDAP 同期を使用して、LDAP 同期によるセキュリティのプロビジョニングを行う場合は、**[電話セキュリティプロファイルタイプ]** で **[Universal Device Template] を選択します。**

ステップ 4 プロファイルの名前を入力します。

ステップ 5 [デバイスのセキュリティモード（Device Security Mode）]ドロップダウンリストから、[暗号化（Encrypted）] または [認証済み（Authenticated）]を選択します。

ステップ 6 (SIP 電話のみ) 転送タイプから、 **TLS** を選択します。

ステップ 7 [電話のセキュリティプロファイルの設定（Phone Security Profile Configuration）]ウィンドウで、残りのフィールドを設定します。フィールドとその設定に関するヘルプは、オンラインヘルプを参照してください。

ステップ 8 **[保存（Save）]** をクリックします。

セキュアフォンプロファイルを電話に追加する

この手順を使用して、TLS が有効な電話セキュリティプロファイルを電話に指定します。

（注） 一度に多数の電話にセキュリティプロファイルを割り当てるには、一括管理ツールを使用して、それらの電話にセキュリティ プロファイルを再割り当てします。

手順

ステップ 1 Cisco Unified CM 管理から、**[デバイス]** > **[電話機]** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 新しい電話機を作成するには、[新規追加] をクリックします。

- **[検索（Find）]** をクリックして検索し、既存のテンプレートを選択します。

ステップ 3 電話のタイプとプロトコルを選択し、**[次へ（Next）]** をクリックします。

ステップ 4 [**端末セキュリティプロファイル**] ドロップダウンリストから、作成したセキュリティプロファイルを電話に指定します。

ステップ 5 次の必須フィールドに値を指定します:

- MAC アドレス
- [デバイス プール（Device Pool）]
- [SIPプロファイル（SIP Profile）]
- [オーナーのユーザID(Owner User ID)]
- [電話ボタンテンプレート(Phone Button Template)]

ステップ 6 [電話の設定（Phone Configuration）]ウィンドウで、残りのフィールドを入力します。 フィールドとその設定に関するヘルプは、オンラインヘルプを参照してください。

ステップ 7 **[保存（Save）]** をクリックします。

セキュア電話プロファイルをユニバーサル デバイス テンプレートに追加する

この手順を使用して、TLS 対応の電話セキュリティ プロファイルをユニバーサル デバイス テンプレートに指定します。 LDAP ディレクトリ同期を構成している場合、機能グループ テンプレートとユーザ プロファイルを通じて、このユニバーサル デバイス テンプレートを LDAP 同期に含めることができます。 同期が行われると、セキュアプロファイルが電話にプロビジョニングされます。

手順

ステップ 1 Cisco Unified CM Administration から、以下を選択します。**ユーザ管理** > **ユーザ/電話追加** > **ユニバーサル端末テンプレート**。

ステップ 2 次のいずれかの手順を実行します。

- [新規追加（Add New）] をクリックして新しいテンプレートを作成します。
- **[検索（Find）]** をクリックして検索し、既存のテンプレートを選択します。

ステップ 3 [**名前**] フィールドにテンプレートの名前を入力します。

ステップ 4 [デバイスプール（Device Pool）]ドロップダウン リストから、デバイス プールを選択します。

ステップ 5 **[端末セキュリティプロファイル（Device Security Profile）]** ドロップダウンリストから、作成した TLS 対応のセキュリティプロファイルを選択します。

（注）

電話セキュリティ プロファイルは、 **Universal Device Template** を端末タイプとして使用して作成されている必要があります。

ステップ 6 **[SIP プロファイル（SIP Profile）]** を選択します。

ステップ 7 **[電話ボタンテンプレート（Phone Button Template）]** を選択します。

ステップ 8 **[ユニバーサルデバイステンプレートの設定（Universal Device Template Configuration）]** ウィンドウで、残りのフィールドを入力します。 フィールドとその設定に関するヘルプは、オンラインヘルプを参照してください。

ステップ 9 **[保存（Save）]** をクリックします。
LDAP ディレクトリ同期にユニバーサル デバイス テンプレートを含めます。 LDAP ディレクトリ同期のセットアップ方法については、『Cisco Unified Communications Manager システム設定ガイド』の「「エンドユーザーの設定」」の部分を参照してください。

TLS の連携動作および制限

この章では、TLS 相互作用と制限に関する情報を提供します。

TLS の連携動作

表 *33 : TLS* の連携動作

機能	データのやり取り
共通基準モード	最小 TLS バージョンの構成と共に、Common Criteria モードを有効にできます。 有効にする場合、アプリケーションは引き続き共通基準の要件に準拠し、TLS 1.0 セキュア接続をアプリケーション レベルで無効にします。 共通基準モードが有効な場合、アプリケーションの最小 TLS バージョンを 1.1 または 1.2 のいずれかとして設定できます。 コモンクライテリアモードの詳細については、『 *Cisco Unified Communications Solutions* コマンドラインインターフェイスリファレンスガイド』の「コモンクライテリアへの準拠」を参照してください。

TLS の制限

次の表では、79xx、69xx、89xx、99xx、39xx、IP Communicator などのレガシー電話に Transport Layer Security (TLS) バージョン 1.2 を実装する際に発生する可能性がある問題を示します。 お使いの電話がこのリリースでセキュア モードをサポートしているかどうかを確認するには、Cisco Unified Reporting の電話機能リスト レポートを参照してください。 レガシー電話の機能制限とこの機能を実装するための回避策を次の表に示します。

（注） 回避策は、影響を受ける機能がシステムで機能するように設計されています。ただし、その機能の TLS 1.2 準拠は保証されません。

表 *34 : Transport Layer Security* バージョン *1.2* の制限

機能	制約事項
暗号化モードの旧型の電話	暗号化モードの旧型の電話は機能しません。 回避策はありません。
認証モードの旧型の電話	認証モードのレガシー電話は機能しません。 回避策はありません。
HTTPSに基づくセキュアな URL を使用する IP 電話サービス。	HTTPS に基づくセキュア URL を使用する IP 電話サービスは機能しません。 IP 電話サービスを使用するための回避策: 基礎となるすべてのサービス オプションに HTTP を使用します。 たとえば、企業ディレクトリとパーソナル ディレクトリです。 ただし、Extension Mobilityなどの機能のために機密データを入力する必要がある場合、HTTPは安全性が低いため、推奨されません、特に機密データを入力する必要がある場合。 HTTP の使用には、次のような欠点があります。 • レガシー電話に HTTP を設定し、サポートされている電話に HTTPS を設定する際のプロビジョニングの課題。 • IP 電話サービスにはレジリエンスがありません。 • IP電話サービスを処理するサーバのパフォーマンスが影響を受ける場合があります。
レガシー電話の Extension Mobility Cross Cluster (EMCC)	EMCC は、TLS 1.2 を使用した従来の電話ではサポートされていません。 回避策: 以下のタスクを完了して EMCC を有効にします。 1. HTTPS の代わりに HTTP 上の EMCC を有効にします。 2. すべての Unified Communications Manager クラスタで混合モードをオンにしてください。 3. すべての Unified Communications Manager クラスタに同じ USB eToken を使用してください。

機能	制約事項
レガシー電話でのローカルに重要な証明書 (LSC)	LSC は従来の電話の TLS 1.2 ではサポートされていません。 結果として、LSC に基づく 802.1x および電話 VPN 認証は利用できません。 802.1x の回避策: 古い電話の EAP-MD5 を使用した MIC またはパスワードに基づく認証。 ただし、これらはお勧めできません。 VPN の回避策: エンドユーザのユーザ名とパスワードに基づく電話 VPN 認証を使用します。
暗号化された Trivial File Transfer Protocol (TFTP) 構成ファイル	暗号化されたトリビアル ファイル転送プロトコル (TFTP) 構成ファイルは、製造元がインストールした証明書 (MIC) があっても、従来の電話の TLS 1.2 ではサポートされていません。 回避策はありません。
CallManager 証明書の更新により、レガシー電話の信頼が失われます。	レガシー電話は、CallManager 証明書が更新されると信頼を失います。 たとえば、証明書を更新した後は、電話は新しい設定を取得できません。 これは Unified Communications Manager 11.5.1 にのみ適用されます。 回避策: 従来の電話の信頼性が失われるのを防ぐには、次の手順を実行します。 1. CallManager 証明書を有効にする前に、**[8.0 以前にロールバックするためのクラスタ（Cluster For Roll Back to Pre 8.0）]** エンタープライズパラメータを **[はい（True）]** に設定します。 既定では、この設定によりセキュリティが無効になります。 2. 一時的に TLS 1.0 を許可します (複数の Unified Communications Manager のリブート)。
サポートされていないバージョンの Cisco Unified Communications Manager に接続する	上位の TLS バージョンをサポートしていない古いバージョン Unified Communications Manager への TLS 1.2 接続は機能しません。 たとえば、 Unified Communications Manager リリース 9.x への TLS 1.2 SIP トランク接続は機能しません。このリリースは TLS 1.2 をサポートしていないためです。 以下のいずれかの回避策を使用できます。 • 接続を有効にするための回避策: 推奨されるオプションではありませんが、セキュアではないトランクを使用することができます。 • TLS 1.2 使用中に接続を有効にする回避策: サポートされていないバージョンを TLS 1.2 をサポートするリリースにアップグレードすることができます。

機能	制約事項
証明書信頼リスト (CTL) クライアント	CTL クライアントは TLS 1.2 をサポートしません。 以下のいずれかの回避策を使用できます。 • CTL クライアントの使用時に TLS 1.0 を一時的に許可し、その後クラスタを Common Criteria モードに移動することができます。最小 TLS を 1.1 または 1.2 に設定する • トークンレス CTL に移行するには、CLI コマンド **utils ctl set-cluster 混合モード** を共通基準モードで使用します。 最小 TLS を 1.1 または 1.2 に設定する
アドレス帳シンクロナイザー	回避策はありません。

Transport Layer Security バージョン 1.2 の影響を受ける Cisco Unified Communications Manager ポート

Unified Communications Manager TLS バージョン 1.2 の影響を受けるポートを次の表に示します:

表 *35 : Transport Layer Security* バージョン *1.2* に適用される *Cisco Unified Communications Manager* ポート

アプリケーション (Application)	プロトコル	宛先/リスナー	通常モードで動作している Cisco Unified Communications Manager			共通基準モードで動作する Cisco Unified Communications Manager		
			最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2	最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2
Tomcat	HTTPS	443	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS v1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
SCCP - SEC - SIG	シグナリング接続コントロール部 (SCCP)	2443	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
CTL-SERV	専用	2444	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2

アプリケーション (Application)	プロトコル	宛先/リスナー	通常モードで動作している Cisco Unified Communications Manager			共通基準モードで動作する Cisco Unified Communications Manager		
			最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2	最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2
コンピュータテレフォニー インテグレーション（CTI）	クイックバッファエンコーディング (QBE)	2749	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
CAPF-SERV	Transmission Control Protocol（TCP）	3804	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
クラスター間検索サービス (ILS)	なし	7501	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
管理 XML (AXL)	シンプルオブジェクトアクセスプロトコル (SOAP)	8443	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
高可用性 - プロキシ (HA プロキシ)	[TCP]	9443	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.2	TLS 1.2
SIP-SIG	Session Initiation Protocol（SIP）	5061 (設定可能)	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
HA プロキシ	[TCP]	6971, 6972	TLS 1.2	TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2

アプリケーション（Application）	プロトコル	宛先/リスナー	通常モードで動作している Cisco Unified Communications Manager			共通基準モードで動作する Cisco Unified Communications Manager		
			最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2	最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2
Cisco Tomcat	HTTPS	8080, 8443	8443:TLS 1.0、TLS 1.1、TLS 1.2	8443:TLS 1.1、TLS 1.2	8443: TLS 1.2	TLS 1.1	8443: TLS 1.1、TLS 1.2	8443: TLS 1.2
Trust Verification Service (TVS)	専用	2445	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2

インスタントメッセージングとプレゼンスサービスのポートに Transport Layer Security バージョン 1.3 が適用される

次の表は、Transport Layer Security バージョン 1.2 が適用される IM and Presence Service ポートの一覧です:

表 *36:* トランスポート レイヤ セキュリティ バージョン *1.2* に適用されるインスタントメッセージング *&* プレゼンスポート

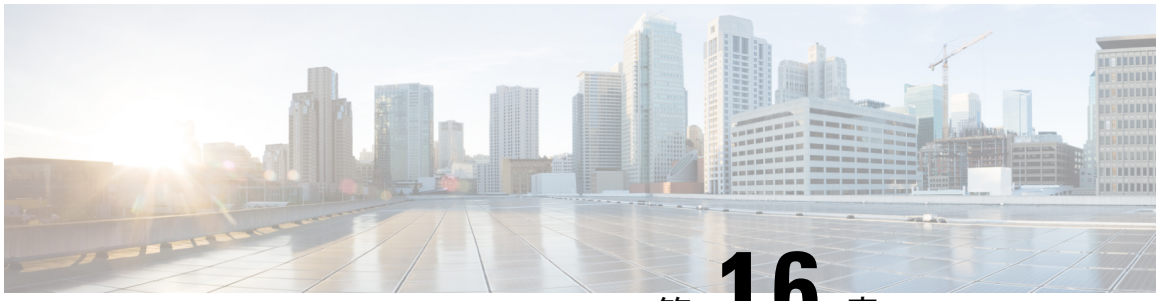
宛先/リスナ	インスタントメッセージおよびプレゼンスは通常モードで動作しています			インスタントメッセージおよびプレゼンスは共通基準モードで動作しています		
	最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2	最小 TLS バージョン 1.0	最小 TLS バージョン 1.1	最小 TLS バージョン 1.2
443	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
5061	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
5062	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2

宛先/リスナ	インスタントメッセージおよびプレゼンスは通常モードで動作しています			インスタントメッセージおよびプレゼンスは共通基準モードで動作しています		
	最小 **TLS** バージョン **1.0**	最小 **TLS** バージョン **1.1**	最小 **TLS** バージョン **1.2**	最小 **TLS** バージョン **1.0**	最小 **TLS** バージョン **1.1**	最小 **TLS** バージョン **1.2**
5280	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
8083	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2
8443	TLS 1.0、TLS 1.1、TLS 1.2	TLS 1.1、TLS 1.2	TLS 1.2	TLS 1.1	TLS 1.1、TLS 1.2	TLS 1.2

第 III 部

ユーザセキュリティ

- アイデンティティ管理 （243 ページ）
- 資格情報ポリシー （251 ページ）
- 連絡先検索認証。 （261 ページ）



第 16 章

アイデンティティ管理

- ユーザセキュリティの概要 （243 ページ）
- ID 管理の概要 （244 ページ）

ユーザセキュリティの概要

ユーザ アクセス

ユーザセキュリティは、脅威をより効率的に関連付けるために、ユーザ、エンドポイント、およびユーザのオンライン活動を保護するプラットフォームで構成されています。個人用デバイスからネットワークにログインするユーザが増加しているため、会社所有のデバイスと同様に個人用デバイスの保護も重要です。

ユーザーとセキュリティの詳細については、『Cisco Unified Communications Manager システム設定ガイド』の「**エンドユーザーの設定**」と、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「**セキュリティの管理**」を参照してください。

エンドユーザを [ロール] に関連付けられたアクセス コントロール グループに割り当て、ユーザ アクセスを管理します Unified Communications Manager。

アクセスコントロールは、適切なユーザによるネットワークへのアクセスを許可する一方で、同時にアクセスしてはならないユーザをブロックします。アクセスコントロールとは、ネットワークにアクセスしている誰と何を可視化する機能のことです。これにより、適切なユーザが適切なデバイスを使用して適切なリソースにアクセスできるようになります。アクセスコントロールは、情報の広がりを規制し、望ましくない訪問者がデータにアクセスするのを防ぎます。

ロールとアクセス コントロール グループは、複数のレベルのセキュリティを Unified Communications Manager に提供します。 各ロールは、Unified Communications Manager 内の特定のリソースに対する権限のセットを定義します。 エンドユーザーをアクセス コントロール グループに指定した後、ロールを割り当てると、エンドユーザーはロールによって定義されたアクセス許可を取得します。

インストール時に、 Unified Communications Manager には定義済みのデフォルトの役割が事前に定義されたアクセスコントロールグループに割り当てられます。エンドユーザをデフォルト

のアクセスコントロールグループに指定したり、新しいアクセスコントロールグループとロールをセットアップしてアクセス設定をカスタマイズすることができます。

ユーザーおよびアクセス制御の詳細は、『Cisco Unified Communications Manager システム設定ガイド』の「**エンドユーザーの設定**」および『Cisco Unified Communications Manager アドミニストレーション ガイド』の「**ユーザーの管理**」を参照してください。

アイデンティティ管理

定義された一連の Cisco アプリケーションのうちの 1 つにサインインした後は、SAML シングル サインオン（SSO）を使用して、それらすべてのアプリケーションにアクセスできます。SAML は信頼できるビジネスパートナー間のセキュリティ関連情報の交換について記述します。 これは、サービス プロバイダー (Cisco Unified Communications Manager など) がユーザを認証するために使用する認証プロトコルです。 SAML では ID プロバイダとサービスプロバイダがセキュリティ認証情報を交換します。 この機能は、さまざまなアプリケーションで共通の資格情報と関連情報を使用するための安全なメカニズムを提供します。 ID 管理の詳細については、「SAML シングルサインオンを管理する Cisco Unified Communications Manager アドミニストレーション ガイド」を参照してください。

連絡先検索認証。

連絡先検索認証では、他のユーザのディレクトリを検索する前に、自分自身を認証する必要があります。 連絡先検索の認証の詳細については、次のトピックを参照してください。

1. 連絡先検索認証のための電話サポートの確認 （262 ページ）
2. 連絡先検索の認証の有効化 （262 ページ）
3. 連絡先検索用のセキュアなディレクトリ サーバの設定 （263 ページ）

ID 管理の概要

Identity Management は Cisco Collaboration の展開に不可欠なコンポーネントです。 アイデンティティはしばしばハッカーの主な標的であるため、システムを安全にするために安全な認証および許可サービスを設定することが不可欠です。 Cisco Unified Communications Manager は、サービスの ID、認証、認可を管理するための多くのオプションを提供します。

- サードパーティ ID プロバイダによる SAML SSO 展開
- LDAP 認証
- ローカル DB 認証

SAML SSO の展開

SAML SSO は生産性を向上させると同時に、エンタープライズのセキュリティを向上させます。 SAML SSO は、SAML 2.0 プロトコルを使用して、Cisco Collaboration インフラストラク

チャをサードパーティの ID プロバイダに接続し、異なるドメインや製品の管理者とクライアントのログインに安全なログインと認証サービスを提供します。 ID プロバイダがシングル ログインを保存するため、Worker の生産性が向上します。一度コラボレーションアプリケーションの 1 つに正常にログインしたら、再度ログインする必要なく、それらのアプリケーションにアクセスできます。

SAML SSO は ID フレームワークに以下の利点を提供します。

- 異なるユーザ名とパスワードの組み合わせを入力する必要性を排除することで、パスワードの手間を軽減します。
- アプリケーションをホストするシステムの認証をサードパーティのシステムに転送します。
- 認証情報を保護および保護します。 SAML SSO は暗号化機能を提供し、IdP、サービスプロバイダー、ユーザ間で受け渡される認証情報を保護します。 SAML SSO は、IdP とサービスプロバイダーの間で受け渡される認証メッセージを外部ユーザから隠すこともできます。
- 同じ ID の資格情報を再入力する時間が短縮されるため、生産性が向上します。
- パスワードのリセットのためのヘルプデスクへの電話が減り、それによりコストが削減され、さらなる節約が可能になります。

IdP との信頼関係

SAML SSO 展開は、サービス プロバイダー (Cisco Unified Communications Manager) とサードパーティのアイデンティティ プロバイダー間の信頼関係の作成に依存しています。 次の 2 つの SSO モードのいずれかを使用して、SAML SSO 関係を設定できます。

- ノードごとの配置—UC メタデータの zip ファイルには、各ノードの個別の XML ファイルが含まれています
- クラスターごとの配置 - クラスターの単一のメタデータ ファイル

この信頼関係は、メタデータ ファイルの最初の交換を通じて作成されます。 Cisco UC メタデータ ファイルは、次の情報を含む XML ファイルです。

- 一意の識別子
- 組織
- この情報の有効期限
- キャッシュ期間
- この情報の XML 署名
- 連絡先担当者
- エンティティの一意の識別子 (エンティティ ID)

- このSAMLインスタンスのSAMLロールの説明(アイデンティティプロバイダ、サービスプロバイダなど)

認証

IdPにより認証が提供されると、Cisco Unified Communications Managerリソースへのユーザアクセスは、ローカルに設定されたアクセスコントロールグループとそれらのグループが提供するロール権限により決定されます。

SAML SSO構成およびIDプロバイダの要件

IDプロバイダの構成情報や要件など、SAML SSOの詳細については、『*Cisco Unified Communications*アプリケーションのための*SAML SSO*導入ガイド』を参照してください。

[LDAP認証(LDAP Authentication)]

SAML SSOを展開しておらず、ユーザを会社のLDAPディレクトリと同期させている場合、LDAP認証により、会社のLDAPディレクトリに保存されている資格情報と照合してユーザのパスワードを認証できます。 このオプションにより、Cisco Unified Communications ManagerのIdentity Management System (IMS) ライブラリが会社のLDAPディレクトリを使用して、LDAP同期ユーザのユーザパスワードを認証できるようになります。

エンドユーザがセルフケアポータルにログインする場合、会社のLDAPディレクトリで設定されている会社のパスワード(ADパスワードなど)を入力します。

このオプションが設定されている場合:

- LDAPからインポートされたユーザのエンドユーザパスワードは、簡単なバインド操作によって、企業ディレクトリに対して認証されます。
- ローカルユーザのエンドユーザパスワードは、Unified CMデータベースに対して認証されます。
- アプリケーションのユーザ パスワードは、Unified CM データベースに対して認証されます。
- エンドユーザの PIN は Unified CM データベースに対して認証されます。

LDAP 認証の設定

この手順を使用して、エンドユーザパスワードのLDAP認証を有効にします。 LDAP認証を既存のLDAPディレクトリ同期に追加できます。

（注） LDAP証明書が更新された場合、管理者はユーザ認証を実行するためにSSOP-Tomcatサービスを再起動する必要があります。

始める前に

この手順は、既存のLDAPディレクトリ同期が設定されていることを前提としています。LDAPディレクトリ同期を設定していない場合は、『Cisco Unified Communications Manager システム設定ガイド』を参照してセットアップします。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム（System）]** > **[LDAP]** > **[LDAP 認証（LDAP Authentication）]**を選択します。

ステップ 2 **[エンドユーザー用 LDAP 認証の使用（Use LDAP Authentication for End Users）]** チェックボックスをチェックします。

ステップ 3 **LDAP マネージャ識別名**には、LDAP マネージャ (問題の LDAP ディレクトリへのアクセス権限を持つ管理ユーザ) のユーザ ID を入力します。

ステップ 4 **パスワード** を入力し、 **パスワードの再確認** を入力します。

ステップ 5 LDAP ディレクトリサーバのアドレス情報を入力します。

ステップ 6 **[LDAP認証の設定（LDAP Authentication Configuration）]** ウィンドウで、残りのフィールドを入力します。

ステップ 7 **[保存（Save）]** をクリックします。

ローカルデータベース認証

サードパーティの ID プロバイダで SAML SSO を展開していない場合、または LDAP 認証が設定されていない場合、エンドユーザには Cisco Unified Communications Manager データベースに対するローカル認証方式が必要です。このオプションでは、ユーザパスワードはローカルデータベースに保存され、[エンド ユーザ設定] で管理されます。

アプリケーションユーザとエンドユーザ PIN の両方について、認証の管理には常にローカルデータベース認証方式が使用されます。次の表では、3 つの主なパスワードタイプとその管理方法を示します。

表 37：

パスワードの種類	資格情報の管理
エンド ユーザー パスワード	SAML SSO または LDAP 認証を使用していない場合、エンドユーザのパスワードは個々のエンドユーザの [エンドユーザの設定] ウィンドウでローカルに管理されます。 すべてのパスワードは [エンドユーザの設定] から更新できます。エンド ユーザはセルフケア ポータルから自分のパスワードを編集できます。

パスワードの種類	資格情報の管理
エンド ユーザ PIN	SAML SSO または LDAP 認証のいずれを展開しているかに関係なく、エンドユーザの PIN は常に Cisco Unified CM Administration の [エンドユーザの構成] ウィンドウで管理されます。 管理者は、[エンドユーザの設定] ウィンドウから既存のエンドユーザ PIN を編集できます。
アプリケーション ユーザー パスワード	SAML SSO または LDAP 認証のどちらを展開しているかに関係なく、アプリケーション ユーザ パスワードはローカル データベースに保存され、Cisco Unified CM Administration の [アプリケーション ユーザの構成] ウィンドウで管理されます。

（注） すべてのローカルパスワードと PIN は暗号化された形式でデータベースに保存されます。

Oauth フレームワーク

OAuth 認証フレームワークは、RFC 6749 に基づいて IETF によって定義されています。OAuth 2.0 認証プロトコルにより、リソース所有者（例えば、Cisco Unified Communications Manager）は、HTTP サービスへの制限付きアクセスを取得するために、サードパーティのアプリケーションを認証できます。 Cisco Unified Communications Manager では、OAuth フレームワークはアクセストークンを使用してアクセスを提供し、トークンの有効期間中、リソースへのアクセスを提供するためにトークンを更新します。 OAuth により、情報にアクセスしようとするときにウェブサイトがパスワードを要求する必要がなくなります。 OAuth では、リソース所有者がクライアントがサーバ上のリソースにアクセスすることを許可します。

Cisco Jabber クライアントは OAuth リフレッシュ ログインを使用して、Cisco Unified Communications Manager からリソースへのアクセスを取得します。 最初のログインの後、OAuth アクセス トークンと更新トークンは、トークンの有効期間中、リソースへのシームレスなアクセスを提供します。

OAuth リフレッシュ ログイン

OAuth リフレッシュ ログインでは、短命のアクセス トークンにより Jabber が認証され、トークンの寿命中、アクセスが提供されます (アクセス トークンのデフォルトの有効期間は 60 分です)。 古いアクセス トークンが期限切れになると、有効期限が長い更新トークンが Jabber に新しいアクセス トークンを提供します。 更新トークンが有効である限り (デフォルトの有効期間は 60 日)、Jabber クライアントは新しいアクセス トークンを動的に取得できるため、ユーザが再認証する必要なく、シームレスなアクセスを提供できます。

OAuth トークンが有効期間の 75% に達するたびに、エンドユーザのアプリケーションは新しいアクセストークンを要求し、CUCM はエンドユーザを認証するための新しいアクセストークンを提供します。 更新トークンが有効期限の 100% に達した場合、新しいアクセス トークンを生成する前に再認証する必要があります。

SIP OAuth モード

SIP OAuth モードは OAuth フレームワークを強化し、SIP 回線の Oauth アクセストークンと更新トークンの使用を可能にします。これにより、Jabber クライアントに LSC 証明書をインストールする必要がなくなります。 SIP OAuth モードでは、CAPF なしで Jabber の安全な署名とメディアが可能です。 トークンの検証は SIP 登録中に完了します。 このモードでは、Jabber は LSC なしでメディアとシグナリングの暗号化を実行でき、Unified CM で混合モードを有効にする必要はありません。

OAuth のキーの再生成

OAuth トークンの署名と暗号化に使用されるキーが危険にさらされていると思われる場合は、次の CLI コマンドを使用して新しいキーを生成します。 署名キーは非対称で RSA ベースであるのに対し、暗号キーは対称キーです。

- キー再生認証暗号化設定
- キー再生認証署名設定

（注） OAuth キーが再生成された場合は、Jabber OAuth ログインが動作するように、すべての IM and Presence ノードで Cisco XCP 認証サービスを再起動する必要があります。

SIP Oauth モードの設定

SIP 回線に Oauth 更新ログインを使用できるように SIP Oauth モードを設定する方法の詳細については、『*Cisco Unified Communications Manager* 機能設定ガイド』の「SIP OAuth モード」の章を参照してください。

既存の OAuth 更新トークンの取り消し

既存の OAuth 更新トークンを取り消すには、AXL API を使用します。 たとえば、ある従業員が退社した場合、この API を使用してその従業員の現在の更新トークンを取り消し、その従業員が新しいアクセストークンを取得したり、企業アカウントへログインできないようにすることができます。 API は、AXL クレデンシャルで保護されている REST ベースの API です。 任意のコマンドライン ツールを使用して API を呼び出すことができます。 次のコマンドは、更新トークンを取り消すために使用できる cURL コマンドの例を示しています。

```
curl -k -u "admin:password" https://<UCMaddress:8443/ssosp/token/revoke?user_id=<end_user>
```

ここで、

- `admin:password` は、Cisco Unified Communications Manager の管理者アカウントのログイン ID とパスワードです。
- `UCMaddress` は、Cisco Unified Communications Manger のパブリッシャ ノードの FQDN または IP アドレスです。
- `end_user` は、更新トークンを取り消すユーザのユーザ ID です。

第 17 章

資格情報ポリシー

- 資格情報ポリシーの概要 （251 ページ）
- デフォルトのクレデンシャル ポリシーの設定 （253 ページ）
- ユーザ資格情報または資格情報ポリシーの編集 （254 ページ）
- PIN同期の有効化 （255 ページ）
- 認証アクティビティのモニタ （257 ページ）
- クレデンシャル キャッシングの設定 （258 ページ）
- セッション終了の管理 （258 ページ）

資格情報ポリシーの概要

資格情報ポリシーは、Unified Communications Manager 内のリソースの認証プロセスを制御します。 資格情報ポリシーは、パスワード要件と、エンドユーザのパスワード、エンドユーザの PIN、アプリケーションユーザのパスワードに対する、失敗したログイン試行、有効期限、ロックアウト期間などのアカウントロックアウトの詳細を定義します。 資格情報ポリシーは、すべてのエンド ユーザ PIN など、特定の資格情報タイプのすべてのアカウントに広く割り当てたり、特定のアプリケーションユーザまたはエンドユーザ向けにカスタマイズしたりできます。

資格情報タイプ

資格情報ポリシーの構成では、新しい資格情報ポリシーを構成し、その新しいポリシーを次の 3 つの資格情報タイプのそれぞれに対するデフォルトの資格情報ポリシーとして適用できます。

- エンド ユーザ PIN
- エンド ユーザー パスワード
- アプリケーション ユーザーパスワード

特定のエンドユーザ PIN、エンドユーザパスワード、またはアプリケーションユーザパスワードに資格情報ポリシーを適用することもできます。

LDAP 認証が有効な場合の資格情報ポリシー

システムが企業ディレクトリを使用する LDAP 認証用に設定されている場合:

- LDAP 認証を有効にすると、資格情報ポリシーはエンドユーザのパスワードに適用されません。
- LDAP 認証が有効になっているかどうかに関係なく、エンドユーザの PIN とアプリケーションユーザのパスワードには資格情報ポリシーが適用されます。 これらのパスワードの種類はローカル認証を使用します。

（注） クレデンシャル ポリシーは、オペレーティング システムのユーザまたは CLI のユーザには適用されません。 オペレーティング システムの管理者は、オペレーティング システムでサポートされている標準のパスワード検証手順を使用します。

単純なパスワード

簡単なパスワードと PIN をチェックするようにシステムを設定することができます。 単純なパスワードとは、簡単にハッキングされる可能性のある認証情報です。たとえば、パスワードに ABCD を使用したり、PIN に 123456 を使用したりといった、簡単に推測できるパスワードです。

簡単でないパスワードは、次の要件を満たします。

- パスワードには、少なくとも 1 つの大文字、1 つの小文字、1 つの数字、および 1 つの特殊文字が含まれている必要があります。
- 1 つの文字または数字を 4 回以上連続して使用しない。
- エイリアス、ユーザ名、内線を繰り返したり、含めたりしない。
- 連続する文字や数字は使用できません。 例えば、654321 や ABCDEFG のようなパスワードは使用できません。

PIN に使用可能な文字は数字（0 ～ 9）だけです。 単純すぎない PIN とは、次の基準を満たす PIN です。

- 同じ数字を 3 回以上連続して使用しない。
- ユーザの内線番号、メールボックス、またはユーザ内線またはメールボックスの逆を繰り返したり、含めたりしてはなりません。
- 3 つの異なる数字を含める必要があります。 たとえば、121212 などの PIN は単純すぎます。
- ユーザの姓または名の数字表現（名前によるダイヤル）と一致させない。
- 数字の繰り返しグループ（408408 など）、およびキーパッドの直線方向にダイヤルされるパターン（2580、159、753 など）を使用しない。

クレデンシャル ポリシーの JTAPI および TAPI のサポート

Cisco Unified Communications Manager Java テレフォニー アプリケーション プログラミング インターフェイス（JTAPI）およびテレフォニー アプリケーションプログラミング インターフェイス（TAPI）は、アプリケーションユーザに割り当てられたクレデンシャル ポリシーをサポートするため、開発者はパスワードの有効期限、PIN の有効期限、およびクレデンシャル ポリシーの適用ためのロックアウト戻りコードに応答するアプリケーションを作成する必要があります。

アプリケーションは、アプリケーションが使用する認証モデルに関係なく、API を使用してデータベースまたは社内ディレクトリで認証します。

開発者向けの JTAPI および TAPI の詳細については、開発者ガイド（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html）を参照してください。

デフォルトのクレデンシャル ポリシーの設定

新しくプロビジョニングされたユーザに適用されるクラスタ全体のデフォルトのクレデンシャル ポリシーを設定するには、この手順を使用します。 次の各クレデンシャル タイプに対して、個別のクレデンシャル ポリシーを適用できます。

- アプリケーション ユーザー パスワード
- エンド ユーザー パスワード
- エンド ユーザ PIN

手順

ステップ 1 クレデンシャル ポリシーの設定を入力します。

a) Cisco Unified CM Administration で、**[ユーザ管理]** > **[ユーザ設定]** > **[クレデンシャル ポリシーのデフォルト]** を選択します。

b) 次のいずれかを実行します。

- [検索（Find）] をクリックし、既存のクレデンシャル ポリシーを選択します。
- [新規追加（Add New）]をクリックして、新しいクレデンシャル ポリシーを作成します。

c) ABCD や 123456 のようなハッキングされやすいパスワードをシステムにチェックさせる場合は、[単純すぎるパスワードのチェック（Check for Trivial Passwords）]チェックボックスをオンにします。

d) [クレデンシャル ポリシーの設定（Credential Policy Configuration）]ウィンドウの各フィールドに入力します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。
e) **[保存]** をクリックします。
f) 他のクレデンシャル タイプ用に別のクレデンシャル ポリシーを作成する場合は、この手順を繰り返します。

ステップ 2 次のいずれかのクレデンシャル タイプにクレデンシャル ポリシーを適用します。

a) Cisco Unified CM Administration で、**[ユーザ管理]** > **[ユーザ設定]** > **[クレデンシャル ポリシーのデフォルト]** を選択します。
b) クレデンシャル ポリシーを適用するクレデンシャル タイプを選択します。
c) [クレデンシャルポリシー（Credential Policy）]ドロップダウンから、このクレデンシャル タイプに適用するクレデンシャル ポリシーを選択します。 たとえば、作成したクレデンシャル ポリシーを選択できます。
d) [クレデンシャルの変更（Change Credential）]フィールドと[クレデンシャルの確認（Confirm Credential）]フィールドの両方にデフォルトのパスワードを入力します。 ユーザが次にログインするときに、これらのパスワードを入力する必要があります。
e) [クレデンシャル ポリシーのデフォルトの設定（Credential Policy Default Configuration）] ウィンドウで、残りのフィールドを設定します。 フィールドとその設定の詳細については、オンライン ヘルプを参照してください。
f) **[保存]** をクリックします。
g) 他のクレデンシャル タイプにクレデンシャル ポリシーを割り当てる場合は、この手順を繰り返します。

（注） また、個々のユーザに対して、**[エンド ユーザの設定]** ウィンドウまたはそのユーザの **[アプリケーション ユーザ設定]** ウィンドウから、特定のユーザクレデンシャルにポリシーを割り当てすることもできます。 クレデンシャル タイプ (パスワードまたは PIN) の隣にある **[クレデンシャルの編集]** ボタンをクリックして、そのユーザの**クレデンシャル設定** を開きます。

ユーザ資格情報または資格情報ポリシーの編集

既存のユーザ資格情報を編集する場合、またはユーザ資格情報に割り当てられているポリシーを編集する場合は、この手順を使用します。 資格情報をリセットした後、ユーザに次回のログイン時に資格情報を更新することを義務付けるなどのルールを適用できます。 次のような場合に、この操作が必要になります。

- ローカル DB 認証が構成されており、エンドユーザのパスワードをリセットしたい場合
- エンドユーザ PIN またはアプリケーションユーザパスワードをリセットしたい
- 特定のユーザの資格情報に割り当てられている資格情報ポリシーを変更したい

手順

ステップ 1 [Cisco Unified CM の管理（Cisco Unified CM Administration）] から、次のいずれかのウィンドウを選択してください。

- エンドユーザーのパスワードと PIN については、**[ユーザー管理（User Management）]** > **[エンドユーザー（End Users）]** を選択してください。
- アプリケーションユーザーのパスワードを設定するには、**[ユーザー管理（User Management）]** > **[アプリケーションユーザー（Application Users）]** を選択します。

ステップ 2 [**検索**] をクリックして適切なユーザを選択します。

ステップ 3 既存のパスワードまたはPINを変更する場合は、新しい認証情報を**[パスワード（Password）]/[パスワードの確認（Confirm Password）]** または **[PIN]/[PINの確認（Confirm PIN）]** フィールドに入力し、**[保存（Save）]** をクリックします。

ステップ 4 ユーザの資格情報に割り当てられている資格情報ポリシーを変更する場合、またはユーザが次回のログイン時に新しいパスワードまたはPINの入力を要求するなどのルールを適用する場合:

a) **[パスワード（Password）]** または **[PIN]** の隣にある **[認証情報の編集（Edit Credential）]** ボタンをクリックします。 そのユーザーの資格情報に対して **[クレデンシャル設定（Credential Configuration）]** ウィンドウが開きます。

b) これはオプションです。 新しい資格情報ポリシーを指定するには、[**認証ルール**] ドロップダウンからポリシーを選択します。

c) これはオプションです。ユーザーの次回のログイン時にパスワードまたはPINを更新するには、**[ユーザーは次回ログイン時に変更する必要あり（User Must Change at Next Login）]** チェックボックスを選択します。

d) 残りのフィールドに入力します。 フィールドの説明については、オンライン ヘルプを参照してください。

e) **[保存（Save）]** をクリックします。

PIN同期の有効化

PIN 同期を有効にし、エンド ユーザが、エクステンション モビリティ、開催中の会議、モバイル コネクト、および Cisco Unity Connection ボイスメールに同じ PIN を使用してログインできるようにするには、次の手順を実行します。

（注） Cisco Unified Communications Manager パブリッシャ データベース サーバが実行されており、そのデータベースのレプリケーションが完了した場合のみ、Cisco Unity Connection と Cisco Unified Communications Manager 間の PIN の同期に成功します。 Cisco Unity Connection で PIN の同期に失敗すると、次のエラー メッセージが表示されます。[CUCMで暗証番号のアップデートに失敗しました。（Failed to update PIN on CUCM.） 原因：PIN の取得中にエラーが発生しています。（Reason: Error getting the pin.）]

PIN 同期が有効で、エンドユーザーが PIN を変更した場合は、Cisco Unified Communications Manager で PIN を更新します。 この現象は、少なくとも 1 つの構成済みの Unity Connection アプリケーション サーバで、PIN の更新が成功している場合に発生します。

（注） PIN の同期を有効にするには、機能が正常に有効化された後で、管理者がユーザに各自の PIN を変更するよう強制する必要があります。

始める前に

この手順では、すでにアプリケーションサーバが Cisco Unity Connection のセットアップに接続されていることを前提としています。使用していない場合、新しいアプリケーションサーバを追加する方法については、「関連項目」を参照してください。

PIN 同期機能を有効にするには、まず Cisco Unified OS Administration ページから Cisco Unified Communications Manager tomcat-trust に、有効な証明書をアップロードする必要があります。 証明書をアップロードする方法の詳細については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）の「「セキュリティ証明書の管理」」の章を参照してください。

Cisco Unity Connection サーバのユーザ ID は、Cisco Unified Communications Manager のユーザー ID と一致する必要があります。

手順

ステップ 1 Cisco Unified CM Administration から、**[システム（System）] > [アプリケーションサーバ（Application Servers）]** を選択します。

ステップ 2 Cisco Unity Connection をセットアップするアプリケーション サーバを選択します。

ステップ 3 [エンドユーザのPIN同期（Enable End User PIN Synchronization）]チェックボックスをオンにします。

ステップ 4 **[保存（Save）]** をクリックします。

関連トピック

アプリケーション サーバの設定

認証アクティビティのモニタ

システムは、最後のハッキング試行時刻や失敗したログイン試行のカウントなどの最新の認証結果を表示します。

システムは、次のクレデンシャル ポリシー イベントに関するログ ファイル エントリを生成します。

- 認証成功
- 認証失敗（不正なパスワードまたは不明）
- 次の原因による認証失敗
  - 管理ロック
  - ハッキング ロック（失敗したログオン ロックアウト）
  - 期限切れソフト ロック（期限切れのクレデンシャル）
  - 非アクティブ ロック（一定期間使用されていないクレデンシャル）
  - ユーザによる変更が必要（ユーザが変更するように設定されたクレデンシャル）
  - LDAP 非アクティブ（LDAP 認証へ切り替えたものの LDAP が非アクティブ）
- 成功したユーザ クレデンシャル更新
- 失敗したユーザ クレデンシャル更新

（注） エンド ユーザ パスワードに対して LDAP 認証を使用する場合は、LDAP は認証の成功と失敗だけを追跡します。

すべてのイベント メッセージに、文字列 「ims-auth」 と認証を試みているユーザ ID が含まれています。

手順

ステップ 1 Cisco Unified CM Administration から、**[ユーザの管理（User Management）]** > **[エンド ユーザ（End Users）]** を選択します。

ステップ 2 検索条件を入力し、[検索（Find）]をクリックして、表示された一覧からユーザを選択します。

ステップ 3 [クレデンシャルの編集（Edit Credential）]をクリックし、ユーザの認証アクティビティを表示します。

次のタスク

Cisco Unified Real-Time Monitoring Tool（Unified RTMT）を使用してログ ファイルを表示できます。 キャプチャされたイベントをレポートに収集することもできます。 Unified RTMT の詳細な使用手順については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』（http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html）を参照してください。

クレデンシャル キャッシングの設定

クレデンシャル キャッシングを有効にすると、システム効率が向上します。 システムは、ログイン要求ごとに、データベース ルックアップを実行したり、ストアド プロシージャを呼び出したりする必要がありません。 キャッシュ期間が経過するまでは、関連付けられているクレデンシャル ポリシーが適用されません。

この設定は、ユーザ認証を呼び出すすべての Java アプリケーションに適用されます。

手順

ステップ 1 Cisco Unified CM Administrationから、**[システム]** > **[企業パラメータ]** を選択します。

ステップ 2 必要に応じて、次のタスクを実行します。

- [キャッシングの有効化（Enable Caching）]エンタープライズパラメータを [True]に設定します。 このパラメータを有効にすると、Cisco Unified Communications Manager は、最大 2 分間、キャッシュされたクレデンシャルを使用します。
- システムがキャッシュされたクレデンシャルを認証に使用しないように、キャッシングを無効にするには、[キャッシングの有効化（Enable Caching）]エンタープライズパラメータを [False]に設定します。 LDAP 認証の場合、この設定は無視されます。 クレデンシャル キャッシングでは、ユーザごとに最小量の追加メモリが必要です。

ステップ 3 **[保存（Save）]** をクリックします。

セッション終了の管理

管理者は、各ノードに固有のユーザのアクティブなサインインセッションを終了するために、次の手順を使用できます。

（注）
- 特権レベル 4 を持つ管理者のみが、セッションを終了できます。
- セッション管理では、特定のノード上のアクティブなサインイン セッションを終了します。 管理者は、異なるノード間ですべてのユーザセッションを終了する場合には、各ノードにサインインしてセッションを終了する必要があります。

これは、次のインターフェイスに適用されます。

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified のレポート
- Cisco Unified Communications セルフ ケア ポータル
- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence のレポート

手順

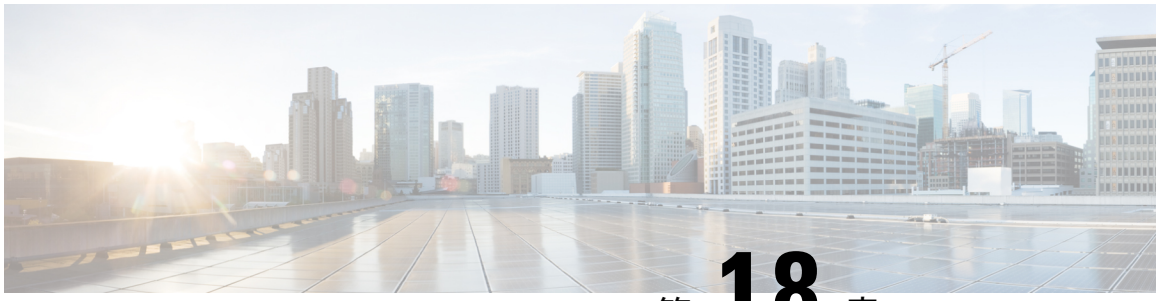
ステップ 1 Cisco Unified OS Administration または Cisco Unified IM and Presence OS Administration から、**[セキュリティ（Security）]** > **[セッション管理（Session Management）]** を選択します。
[セッション管理（Session Management）] ウィンドウが表示されます。

ステップ 2 [ユーザ ID（User ID）] フィールドにアクティブなサインイン ユーザのユーザ ID を入力します。

ステップ 3 [セッションの終了（Terminate Session）] をクリックします。

ステップ 4 **OK**をクリックします。

終了したユーザは、サインインしたインターフェイス ページを更新にすると、サインアウトします。 監査ログにエントリが作成され、そこに終了した `userID` が表示されます。



第 18 章

連絡先検索認証。

- 連絡先検索の認証の概要 （261 ページ）
- 連絡先検索の認証タスクフロー （261 ページ）

連絡先検索の認証の概要

連絡先検索認証は、会社のディレクトリにアクセスするユーザが自身を認証する必要があることを確認することで、システムのセキュリティを強化します。 この機能により、外部関係者によるディレクトリへのアクセスを保護できます。

連絡先検索の認証タスクフロー

以下のタスクを完了して、Unified Communications Manager で連絡先検索の認証をセットアップします。 この機能が設定されている場合、ユーザはディレクトリで他のユーザを検索する前に自分自身を認証する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	連絡先検索認証のための電話サポートの確認 （262 ページ）	お使いの電話がこの機能に対応していることを確認してください。 Cisco Unified Reporting の **Unified CM Phone 機能リスト** レポートを実行して、この機能をサポートする電話モデルのリストを取得してください。
ステップ 2	連絡先検索の認証の有効化 （262 ページ）	連絡先検索認証のために Unified Communications Manager を設定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 3	連絡先検索用のセキュアなディレクトリサーバの設定 （263 ページ）	電話ユーザがディレクトリで他のユーザを検索する際に転送される URL を Unified Communications Manager に設定するには、この手順を使用します。

連絡先検索認証のための電話サポートの確認

導入中の電話が連絡先検索認証をサポートしていることを確認してください。 電話機能リストレポートを実行して、この機能をサポートする電話モデルの完全なリストを取得します。

手順

ステップ 1 Cisco Unified Reporting から **[システムレポート（System Reports）]** をクリックします。
ステップ 2 **[Unified CM 電話機能（Unified CM Phone Feature）]** を選択します。
ステップ 3 **[Unified CM 電話機能（Unified CM Phone Feature）]** レポートをクリックします。
ステップ 4 **[製品（Product）]** フィールドはデフォルト値のままにしておいてください。
ステップ 5 **機能** ドロップダウンから **Authenticated Contact 検索**を選択します。
ステップ 6 [送信（Submit）]をクリックします。

連絡先検索の認証の有効化

電話ユーザの連絡先検索の認証を設定するには、Unified Communications Manager でこの手順に従います。

手順

ステップ 1 コマンドライン インターフェイスにログインします。
ステップ 2 **utils contactsearchauthentication status** コマンドを実行し、このノードの連絡先検索の認証の設定を確認します。
ステップ 3 連絡先検索の認証の設定が必要な場合、

- 認証を有効にするには、**utils contactsearchauthentication enable** コマンドを実行します。
- 認証を無効にするには、**utils contactsearchauthentication disable** コマンドを実行します。

ステップ 4 すべての Unified Communications Manager クラスタ ノードに対してこの手順を繰り返します。

（注）

変更を有効にするには、電話をリセットする必要があります。

連絡先検索用のセキュアなディレクトリ サーバの設定

UDS がユーザの検索要求を送信する先のディレクトリサーバ URL を Unified Communications Manager に設定するには、この手順を使用します。 デフォルト値は `https://<cucm-fqdn-or-ip>:port/cucm-uds/users` です。

（注） 既定の UDS ポートは 8443 です。連絡先検索認証が有効になると、既定の UDS ポートは 9443 に切り替わります。その後、連絡先検索認証を無効にした場合、手動で UDS ポートを 8443 に戻す必要があります。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから **システム** > **エンタープライズパラメータを選択します**。

ステップ 2 [Secure Contact Search URL] テキスト ボックスに、セキュアな UDS ディレクトリ要求の URL を入力します。

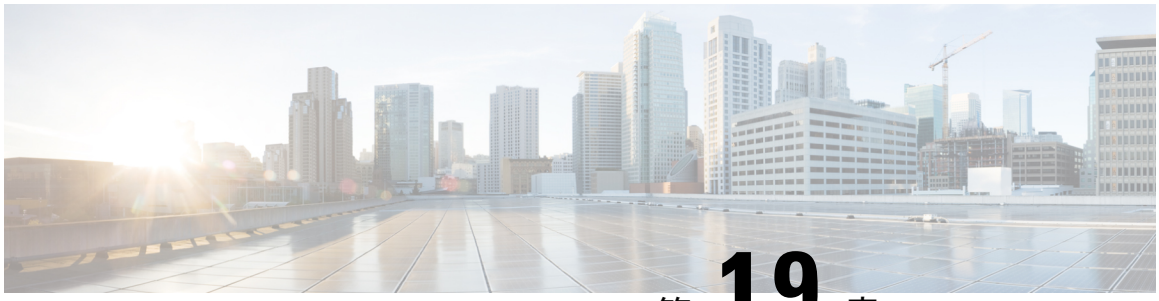
（注）
URL には、Cisco TFTP サービスを実行していないノードを選択することを推奨します。 Cisco TFTP と UDS サービスのいずれかのサービスが再起動すると、互いに悪影響が及ぶ可能性があります。

ステップ 3 **[保存（Save）]** をクリックします。

第 IV 部

高度なシステムセキュリティ

- FIPS モードのセットアップ （267 ページ）
- 共通基準認定ソリューションの ECDSA サポート （281 ページ）
- V.150 の最小必須要件 （287 ページ）
- IPSec のセットアップ （299 ページ）
- CTI、JTAPI、および TAPI の認証と暗号化のセットアップ （301 ページ）
- 安全な録画とモニタリング （317 ページ）
- VPN クライアント （319 ページ）
- オペレーティング システムとセキュリティ強化 （335 ページ）



第 19 章

FIPS モードのセットアップ

- FIPS セットアップ （267 ページ）
- 強化されたセキュリティ モード （273 ページ）
- 共通基準モード （276 ページ）

FIPS セットアップ

⚠

注意 FIPS モードは FIPS 準拠のリリースでのみサポートされます。 警告: 非 FIPS 準拠バージョンにアップグレードする前に、FIPS モードを無効にする必要があることに注意してください Unified Communications Manager。

どのリリースが FIPS に準拠しているか、およびそれぞれの認証を確認するには、 *FIPS 140* のドキュメント (https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html) を参照してください。

FIPS (連邦情報処理標準) は、米国およびカナダの政府認証標準です。 暗号モジュールが従わなければならない要件を定義します。

Unified Communications Manager の特定のバージョンは、米国国立標準技術研究所（NIST）による FIPS 140-2 に準拠しています。 FIPS モード、レベル 1 準拠で動作できます。

Unified Communications Manager

- 再起動
- 起動時に証明書のセルフテストを実行する
- 暗号モジュールの整合性チェックを実行します
- 鍵材料を再生成する

FIPS 140-2 モードを有効にした場合。 この時点で、 Unified Communications Manager は FIPS 140-2 モードで動作します。

FIPS 要件には以下が含まれます。

- 起動時のセルフテストの実行
- 承認された暗号化関数のリストに対する制限

FIPS モードは、以下の FIPS 140-2 レベル 1 検証済み暗号モジュールを使用します。

（注） 次のリストは 12.5(1)SU1-SU5 および 14 のみで利用可能です。

- CiscoSSL 1.0.2n.6.2.194 (FIPS モジュール付き) CiscoSSL FOM 6_2_0
- CiscoJ 5.2.1
- RSA CryptoJ 6_2_3
- OpenSSH 7.5.9
- Libreswan
- NSS

- CiscoSSL 1.0.2zb.6.2.438 FIPS モジュールと共に CiscoSSL FOM 6_2_0
- CiscoJ 5.3.7
- RSA CryptoJ 6_2_3
- OpenSSH 7.5.14i
- Libreswan
- NSS

以下の FIPS 関連のタスクを実行することができます:

- FIPS 140-2 モードを有効にする
- FIPS 140-2 モードを無効にする
- FIPS 140-2 モードのステータスを確認する

（注）
- デフォルトでは、システムは非FIPSモードになっています。 有効にする必要があります。
- クラスタを FIPS、Common Criteria、または Enhanced Security モードにアップグレードする前に、セキュリティパスワードの長さが 14 文字以上であることを確認してください。前のバージョンがFIPSに対応していた場合でも、パスワードを更新する必要があります。

FIPS モードで自己署名証明書または証明書署名リクエスト CSR を生成する場合、証明書は SHA256 ハッシュアルゴリズムを使用して暗号化する必要があり、SHA1 を選択することはできません。

FIPS 140-2 モードを有効にする

Unified Communications Managerで FIPS 140-2 モードを有効にする前に、次のことを考慮してください:

- 非 FIPS モードから FIPS モードに切り替えると、MD5 および DES プロトコルは機能しなくなります。
- 単一サーバ クラスタでは、証明書が再生成されるため、FIPS モードを有効にする前に、CTL クライアントを実行するか、Prepare Cluster for Rollback to pre-8.0 エンタープライズ パラメータを適用する必要があります。 これらの手順のいずれかを実行しない場合、FIPS モードを有効にした後に手動で ITL ファイルを削除する必要があります。
- クラスターでは、すべてのノードが FIPS または非 FIPS モードのいずれかである必要があります。 各ノードを異なるモードにすることはできません。 たとえば、FIPS モードのノード A と非 FIPS モードのノード B は許可されません。
- サーバで FIPS モードを有効にした後は、サーバが再起動して電話が正常に再登録されるまで待ってから、次のサーバで FIPS を有効にしてください。

注意 FIPS モードを有効にする前に、システムのバックアップを実行することを強く推奨します。起動時に FIPS チェックが失敗すると、システムが停止し、リカバリ CD の復元が必要になります。

展開時にすべてのクラスターノードが FIPS モードまたは非 FIPS モードに設定されていることを確認してください。 クラスター内に混合ノードを展開することはできません。 クラスターは FIP または非 FIPS ノードのいずれかである必要があります。

手順

ステップ 1 CLI セッションを開始してください。

詳細については、『「Cisco Unified コミュニケーションソリューション用コマンドラインインタフェースリファレンスガイド』の」 CLI セッションの開始 を参照してください。

ステップ 2 **重要**
この手順は、15SU3 より下のリリースにのみ適用されます。 リリース 15SU3 以降の場合はこの手順をスキップしてください。

CLI で、 **utils fips disable と入力します。**

14 文字未満のパスワードを入力すると、次のプロンプトが表示されます。

```
FIPS、共通基準、セキュリティ強化モードなどのセキュリティモードを有効にする前に、クラスターセキュリティパスワードは14文字以上でなければなりません。 すべてのノードで「set password user
```

```
 security」CLI コマンドを使用してクラスター セキュリティ パスワードを更新し、このコマンドを再試行します。
**************************************************************************
 コマンドの実行に失敗しました
```

14 文字を超えるパスワードを入力すると、次のプロンプトが表示されます。

```
セキュリティ警告: この操作では次の証明書が再生成されます: 1)CallManager 2)Tomcat 3)IPsec 4)TVS 5)CAPF 6)SSH 7)ITLRecovery 上記のコンポーネント用にアップロードされたサードパーティ CA 署名付き証明書は、再アップロードする必要があります。 システムが混合モードで動作している場合、CTL クライアントを再度実行して、CTL ファイルを更新する必要があります。 クラスター内に他のサーバがある場合は、このノードでの FIPS 操作が完了し、システムが再起動し、正常に動作するまで、他のノードの FIPS 設定を変更しないでください。 エンタープライズ パラメータ「TFTP ファイル署名アルゴリズム」が、Unified Communications Manager の現在のバージョンでは FIPS に準拠していない値「SHA-1」に設定されている場合、署名操作は引き続き成功しますが、完全に FIPS に準拠するために、パラメータ値を SHA-512 に変更することをお勧めします。 SHA-512 を署名アルゴリズムとして設定すると、クラスター内でプロビジョニングされたすべての電話が、SHA-512 署名済み設定ファイルを検証できるようになります。さもないと、電話の登録が失敗する可能性があります。 詳細については、『Cisco Unified Communications Manager セキュリティガイド』を参照してください。
**************************************************************************
 これによりシステムが FIPS モードに変更され、再起動されます。
**************************************************************************
 警告: 続行したら Ctrl+C を押さないでください。 この操作の開始後にキャンセルすると、システムの整合性が失われます。復元するには、システムを再起動して「utils fips ステータス」を実行する必要があります。
**************************************************************************
 続行しますか (はい/いいえ)?
```

ステップ 3 「はい」と入力してください。

次のメッセージが表示されます。

```
証明書を生成しています... オペレーティングシステムで FIPS モードを設定しています。 FIPS モードの有効化に成功しました。
********************************************************** システムを再起動した後は、システムのバックアップを実行することを強く推奨します。 システムは数分以内に再起動されます。
```

Unified Communications Manager 自動的に再起動します。

（注）

- 証明書と SSH キーは、FIPS 要件に従って、自動的に再生成されます。
- 単一サーバ クラスタがあり、FIPS 140-2 モードを有効にする前に **Prepare Cluster for Rollback to pre-8.0** エンタープライズ パラメータを適用した場合は、すべての電話がサーバに正常に登録されたことを確認してから、このエンタープライズパラメータを無効にする必要があります。
- クラスターで FIPS を有効にするには、まずパブリッシャを有効にし、構成されたすべてのサービスが適切に初期化され、立ち上がるまでに時間がかかることを確認します。 次に、クラスター内の他のすべてのノードで 1 つずつ、fips を有効にします。

（注）
FIPS モードで、 Unified Communications Manager は、ラクーン (非 FIPS 検証済み) の代わりに LibresWAN (FIPS 検証済み) を使用します。 Racoon のセキュリティポリシーに FIPS が承認していない機能が含まれている場合、CLI コマンドは FIPS が承認した機能を含むセキュリティポリシーを再定義し、中止するように要求します。 詳細については、Cisco Unified Communications Manager アドミニストレーションガイドのメディアリソース管理に関連するトピックを参照してください。

CiscoSSH サポート

Unified Communications Manager は CiscoSSH をサポートしています。 システムで FIPS モードを有効にすると、CiscoSSH が自動的に有効になり、追加の設定は必要ありません。 詳細については、『Cisco Unified Communications Manager と IM and Presence Service の互換性マトリックス』を参照してください。 https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-device-support-tables-list.html

FIPS 140-2 モードを無効にする

Unified Communications ManagerFIPS 140-2 モードを無効にする前に、次の情報を考慮してください:

- 単一または複数のサーバクラスタでは、CTL クライアントを実行することを推奨します。CTL クライアントが単一サーバ クラスターで実行されていない場合、FIPS モードを無効にした後で、ITL ファイルを手動で削除する必要があります。
- 複数サーバクラスターでは、各サーバを個別に無効にする必要があります。FIPS モードはクラスター全体ではなくサーバごとに無効化されるためです。

FIPS 140-2 モードを無効にするには、以下の手順を実行します。

手順

ステップ 1 CLI セッションを開始します。

詳細については、『*Cisco Unified Communications Solutions* 用コマンドラインインターフェイス リファレンスガイド』の「*CLI* セッションの開始」セクションを参照してください。

ステップ 2 CLI で、 **utils fips disable** と入力します。

Unified Communications Manager はリブートし、非 FIPS モードに復元されます。

（注）
証明書と SSH キーは自動的に再生成されます。

FIPS 140-2 モードのステータスの確認

FIPS 140-2 モードが有効になっているかどうかを確認するには、CLI からモードのステータスを確認します。

FIPS 140-2 モードのステータスを確認するには、以下の手順を実行します。

手順

ステップ 1 CLI セッションを開始します。

詳細については、『*Cisco Unified Communications Solutions* 用コマンドラインインターフェイスリファレンスガイド』の「*CLI* セッションの開始」セクションを参照してください。

ステップ 2 CLI で、 **utils fips status** を入力します

FIPS 140-2 モードサーバの再起動

各 FIPS 140-2 モジュールの FIPS スタートアップセルフテストは、再起動後に FIPS 140-2 モードで Unified Communications Manager サーバーが再起動するとトリガーされます。

注意 これらのセルフテストのいずれかが失敗した場合、 Unified Communications Manager サーバは停止します。

（注） Unified Communications Manager サーバは、FIPS が対応する CLI コマンドで有効または無効になると自動的に再起動されます。 リブートを開始することもできます。

注意 一時的なエラーのためにスタートアップのセルフテストに失敗した場合、Unified Communications Managerサーバを再起動することで解決します。 しかし、起動時のセルフテストエラーが解消されない場合は、FIPSモジュールに重大な問題があることを示しており、リカバリ CD を使用する以外に選択肢はありません。

FIPS モードの制限

機能	制約事項
SNMP v3	FIPS モードは、MD5 または DES を使用した SNMP v3 をサポートしていません。 FIPS モードが有効になっている間に SNMP v3 を構成する場合、認証プロトコルとして **SHA** を、プライバシープロトコルとして **AES128** を構成する必要があります。
証明書のリモート登録	FIPS モードは証明書のリモート登録をサポートしていません。
SFTP サーバ	すべての SFTP クライアント（例えば、DRS および CDR）接続は、次のホストキーアルゴリズムを使用します。 • FIPS モードは **rsa-sha2-256 のみをサポートします** • 非 FIPS モードは、**ssh-rsa** のみをサポートします **rsa-sha2-256** (SHA256WithRSA) サポートは OpenSSH 6.8 バージョン以降でのみ利用できます。
IPSec ポリシー	共通基準 (CC) モードでは、証明書ベースの IPSec ポリシーを構成する前に、まずクラスタ/ノード間で証明書の交換を行うことをお勧めします。 証明書ベースの IPSec ポリシーは、非 FIPS から FIPS/Common Criteria モードに、またはその逆に移行する場合には機能しません。 非 FIPS モードから FIPS / CC モード (またはその逆) に移行する必要がある場合は、以下を実行します。 証明書ベースの IPSec ポリシーがあり、有効な状態である場合、 1. FIPS/CC モードに移行する前に、またはその逆に移行する前に、IPSec ポリシーを無効にします。 2. FIPS/CC モードに移行した後、証明書を再認証し、新しい証明書を交換します（その逆も同様です）。 3. IPSec ポリシーを有効にします。

強化されたセキュリティ モード

強化されたセキュリティモードは FIPS 対応システムで実行されます。 Unified Communications Manager と IM and Presence Service の両方は、強化されたセキュリティモードで動作させることができます。これにより、システムに以下のセキュリティおよびリスク管理コントロールを適用することができます。

- ユーザパスワードとパスワード変更に対して、より厳格な資格情報ポリシーが実装されます。
- 連絡先検索の認証機能がデフォルトで有効になります。
- リモート監査ログのプロトコルが TCP または UDP に設定されている場合、デフォルトのプロトコルは TCP に変更されます。 リモート監査ログのプロトコルが TLS に設定されている場合、デフォルトのプロトコルは TLS のままです。 共通基準モードでは、厳格なホスト名検証が実装されています。そのため、証明書と一致する完全修飾ドメイン名(FQDN)でサーバを構成する必要があります。

Unified Communications Manager が FIPS モードの場合、バックアップ端末として設定する端末は FIPS に準拠している必要があります。 鍵交換アルゴリズム **Diffie-hellman-group1-sha1** は FIPS モードではサポートされていません。 **diffie-hellman-group1-sha1** アルゴリズムを Unified Communications Manager の非 FIPS モードに設定すると、FIPS モードを有効にしたときに、このアルゴリズムは自動的に SSH キー交換から削除されます。

資格情報ポリシーの更新

強化されたセキュリティモードが有効になっている場合、新しいユーザパスワードとパスワードの変更には、より厳格な資格情報ポリシーが適用されます。強化型セキュリティモードが有効になった後で、管理者は **set password ***** 一連の CLI コマンドを使用して、これらの要件を変更できます。

- パスワードの長さは 14 から 127 文字の間でなければなりません。
- パスワードには、少なくとも 1 個の小文字、1 個の大文字、1 個の数字、および 1 個の特殊文字が必要です。
- 過去 24 個のパスワードの再使用は許可されません。
- パスワードの最短寿命は 1 日、最長寿命は 60 日です。
- 新しく生成されるパスワードの文字列は、古いパスワードの文字列と少なくとも 4 文字異なる必要があります。

（注） Unified Communications Manager が拡張モードで動作する場合、IPMASysUser および IPMASecureSysUser のユーザー資格情報を必ず変更してください。 そうしないと、IPMA 機能が稼働状態にならず、「IPMANotStarted」アラームがトリガーされます。 次の Cisco Tomcat サービス再起動時または IPMA サービス再起動時に、CLI セッションが一杯になります。

アプリケーションユーザーのパスワードサインイン情報は、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「アプリケーション ユーザー パスワード クレデンシャル情報の管理」の項に記載されている方法で変更できます。

Cisco Unified CM Administration ユーザーインターフェイスから、**ユーザー管理（User Management）> アプリケーションユーザー（Application User）]** に移動して、**[クレデンシャルの編集（Edit Credential）]** をクリックします。 認証ルールのドロップダウンリストで、**[拡張セキュリティ資格情報ポリシー（Enhanced Security Credential Policy）]** を選択し、**[ユーザは次回ログイン時に変更する必要あり（User Must Change at Next Login check box）]** チェックボックスがオフになっていることを確認します。 「資格情報ポリシーの更新」セクションで説明されているように、強化されたセキュリティ モード ポリシーを表示できます。

セキュリティ強化モードを設定する

セキュリティ強化モードを有効にする前に、FIPS を有効にします。

すべての Unified Communications Manager または IM and Presence Service クラスタノードでこの手順を使用してセキュリティ強化モードを設定します。

（注） セキュリティ強化モードを有効にした後に IM and Presence Service パブリッシャーでパスワードを変更する場合、 Unified Communications Manager パブリッシャーのサービスが「開始済み」状態であることを確認する必要があります (「Cisco IM and Presence Data Monitor」サービスおよび SyncAgent)。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 **utils EnhancedSecurityMode status** コマンドを実行し、セキュリティ強化モードが有効になっているかどうか確認してください。

ステップ 3 Unified Communications Manager クラスターノードで次のいずれかのコマンドを実行します:

- 強化されたセキュリティモードを有効にするには、 **utils EnhancedSecuritymode enable** コマンドを実行します。
- 強化されたセキュリティモードを有効にするには、 **utils EnhancedSecuritymode enable** コマンドを実行します。

ステップ 4 強化されたセキュリティモードを有効にしたら、Cisco Unified CM Administration のユーザインターフェイスで、14 文字を含む新しいパスワードに変更します。

Unified Communications Manager パブリッシャーで強化されたセキュリティモードを有効にした後、次の操作を行います:

1. Unified Communications Manager 登録者で強化型セキュリティモードを有効にしてください。
2. IM and Presence Service パブリッシャーで強化されたセキュリティモードを有効にしてください。
3. IM and Presence Service 登録者で強化型セキュリティモードを有効にしてください。

（注）
すべてのノードで、 **utils EnhancedSecurityMode enable** または **utils EnhancedSecurityMode disable** CLI コマンドを同時に実行しないでください。

共通基準モード

共通基準モードにより、 Unified Communications Manager と IM and Presence Service サービスが共通基準ガイドラインに準拠できるようになります。 共通基準モードは、各クラスター ノードで以下の CLI コマンド セットを使用して構成できます。

- `utils fips_common_criteria enable`
- `utils fips_common_criteria 無効`
- `utils fips_common_criteria ステータス`

コモンクライテリア設定タスクフロー

- 共通基準モードを有効にするには、FIPS モードが実行されている必要があります。 FIPS がまだ有効になっていない場合、コモン クライテリア モードを有効にしようとすると、有効にするようにプロンプトが表示されます。 FIPS を有効にするには、証明書の再生成が必要です。 詳細については、FIPS 140-2 モードを有効にする （269 ページ）を参照してください。
- 共通基準 (CC) モードでは、証明書ベースの IPSec ポリシーを構成する前に、まずクラスタ/ノード間で証明書の交換を行うことをお勧めします。
- 共通基準モードでは X.509 v3 証明書が必要です。 X.509 v3 証明書により、以下の通信プロトコルとして TLS 1.2 を使用する際の安全な接続が可能になります。
  - リモート監査のログ記録
  - FileBeat クライアントと logstash サーバ間の接続を確立しています。

Unified Communications Manager と IM and Presence Service を共通基準モードに設定するには、次を実行します:

手順

	コマンドまたはアクション	目的
ステップ 1	[VLANの有効化（Enable TLS）]（277 ページ）	TLS は共通基準モードを構成するための前提条件です。
ステップ 2	共通基準モードを設定する （278 ページ）	すべての Unified Communications Manager および IM and Presence Service クラスタノードに Common Criteria モードを設定する。

[VLANの有効化（Enable TLS）]

TLS 1.2 バージョンまたは TLS バージョン 1.1 は共通基準モードの要件です。 コモンクライテリアモードを有効にすると、TLS バージョン 1.0 を使用した安全な接続は許可されなくなります。

- TLS 接続の確立中に、ピア証明書の `extendedKeyUsage` 拡張機能の値が適切であるかどうかがチェックされます。
  - ピアがサーバの場合、ピア証明書には `serverAuthextendedKeyUsage` 拡張機能が必要です。
  - ピアがサーバの場合、ピア証明書には `serverAuthextendedKeyUsage` 拡張機能が必要です。

`extendedKeyUsage` 拡張機能がピア証明書に存在しないか、適切に設定されていない場合、接続は閉じられます。

TLS バージョン 1.2 をサポートするには、以下を実行します。

手順

ステップ 1 Soap UI バージョン 5.2.1 をインストールします。

ステップ 2 Microsoft Windows プラットフォームを実行している場合:

a) `C:\Program Files\SmartBear\SoapUI-5.2.1\bin` に移動します。

b) `SoapUI-5.2.1.vmoptions` ファイルを編集して、`-Dsoapui.https.protocols=TLSv1.2,TLSv1,SSLv3` を追加し、ファイルを保存します。

ステップ 3 Linux を実行している場合は、`bin/soaup.sh` ファイルを編集して `JAVA_OPTS="$JAVA_OPTS -Dsoapui.https.protocols=SSLv3,TLSv1.2"` と入力し、ファイルを保存します。

ステップ 4 OSX を実行している場合:

a) /Applications/SoapUI-{VERSION}.app/Contents に移動します。
b) SoapUI-5.2.1.vmoptions ファイルを編集して、
-Dsoapui.https.protocols=TLSv1.2,TLSv1,SSLv3 を追加し、ファイルを保存します。

ステップ 5 SoapUI ツールを再起動し、AXL テストを続行します

共通基準モードを設定する

この手順を使用して、 Unified Communications Manager および IM and Presence Service サービスの共通基準モードを設定します。

手順

ステップ 1 コマンドラインインターフェースのプロンプトにログインします。

ステップ 2 utils fips_common_criteria status コマンドを実行して、システムが Common Criteria モードで動作しているかどうかを確認します。

ステップ 3 クラスター ノードで以下のいずれかのコマンドを実行します。

- コモンクライテリアモードを有効にするには、utils fips_common_criteria enable を実行します。
- コモンクライテリアモードを有効にするには、utils fips_common_criteria disable を実行します。

  共通基準モードが無効になっている場合、最小の TLS バージョンを設定するためのプロンプトが表示されます。

（注）
すべてのノードでこれらのコマンドを同時に実行しないでください。

ステップ 4 単一クラスタ全体で共通基準モードを有効にするには、すべての Unified Communications Manager [適切な用語] IM and Presence Service クラスタノードでこの手順を繰り返します。

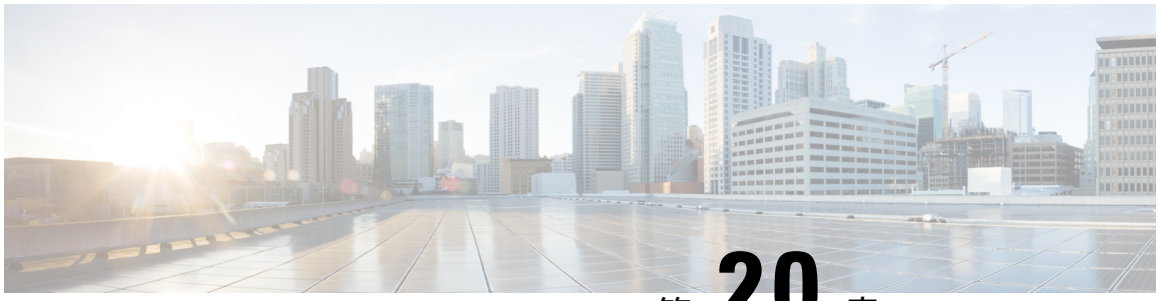
（注）
- CTL クライアントは Unified Communications Manager ノードに接続しません。サーバが Common Criteria モードの場合、CTL クライアントは TLS 1.1 および TLS 1.2 プロトコルをサポートしないためです。
- DX シリーズおよび 88XX シリーズ電話など、TLS 1.1 または TLS 1.2 をサポートする電話モデルのみが、Common Criteria モードでサポートされます。 7975 および 9971 など、TLSv1.0 のみをサポートする電話モデルは、Common Criteria モードでサポートされません。
- CTL クライアントの使用時に TLS 1.0 を一時的に許可し、その後クラスタを Common Criteria モードに移動することができます。 最小 TLS を 1.1 または 1.2 に設定します。

- トークンレス CTL に移行するには、CLI コマンド **utils ctl set-cluster 混合モード** を共通基準モードで使用します。 最小 TLS を 1.1 または 1.2 に設定します。

ステップ 5 ノード間で ICSA がすでに構成されているマルチクラスターセットアップでコモンクライテリアモードを有効にするには、以下の順序で各ノードでコモンクライテリアモードを有効にします。

1. Unified Communications Manager - クラスター 1 (パブリッシャー)
2. IM and Presence Service - クラスター 1 (パブリッシャー)
3. IM and Presence Service - クラスター 1 (サブスクライバーまたはサブスクライバー)
4. Unified Communications Manager - クラスター 2 (パブリッシャー)
5. IM and Presence Service - クラスター 2 (パブリッシャー)
6. IM and Presence Service - クラスター 2 (サブスクライバーまたはサブスクライバー)

ステップ 6 証明書の同期に失敗した場合は、該当のリソースを参照してください。



第 20 章

共通基準認定ソリューションの ECDSA サポート

• ECDSA による認定ソリューションの Common Criteria サポート （281 ページ）

ECDSA による認定ソリューションの Common Criteria サポート

Unified Communications Manager は、楕円曲線デジタル署名アルゴリズム (ECDSA) 証明書をサポートしています。 これらの証明書は RSA ベースの証明書より強力で、Common Criteria (CC) 認証を持つ製品に必要です。 CSfC（米国政府機関向け商用ソリューション）プログラムは、CC 認定を必要とします。そのため、それは Unified Communications Manager に含まれています。

ECDSA 証明書は、次の領域で既存の RSA 証明書と一緒に入手できます。証明書マネージャ、SIP、認証局プロキシ機能 (CAPF)、トランスポート層セキュリティ (TLS) トレース、エントロピー、HTTP、およびコンピュータ テレフォニー インテグレーション (CTI) マネージャ。

（注） ECDSA は、 Unified Communications Manager と Tomcat でのみサポートされています。

Certificate Manager の ECDSA サポート

Unified Communications Manager リリース 11.0 では、証明書マネージャは自己署名 ECDSA 証明書の生成と ECDSA CSR の両方をサポートしています。 Unified Communications Manager の以前のリリースでは、**[RSA]** 証明書のみをサポートしていました。 ただし、Unified Communications Manager リリース 11.0 以降、既存の **[RSA]** 証明書に加えて、 **CallManager-ECDSA** 証明書が追加されました。

CallManager および **CallManager-ECDSA** 証明書は共通の証明書トラストストアである CallManager-Trust を共有します。 Unified Communications Manager はこれらの証明書をこの信頼ストアにアップロードします。

証明書マネージャは、異なるキーの長さの値を持つ ECDSA 証明書の生成をサポートしています。

Unified Communications Manager を更新またはインストールすると、自己署名証明書が生成されます。 Unified Communications Manager リリース 11.0 は常に ECDSA 証明書を持ち、SIP インターフェイスでその証明書を使用します。 セキュアなコンピュータテレフォニーインテグレーション（CTI）マネージャインタフェースは、ECDSA 証明書もサポートしています。 CTI マネージャと SIP サーバは両方とも同じサーバ証明書を使用するため、両方のインターフェイスは同期して機能します。

SIP ECDSA サポート

Unified Communications Manager リリース 11.0 には、SIP 回線および SIP トランク インターフェイスの ECDSA サポートが含まれています。 Unified Communications Manager とエンドポイントの電話またはビデオ端末間の接続は SIP 回線接続であり、2 つの Unified Communications Manager 間の接続は SIP トランク接続です。 すべての SIP 接続は ECDSA 暗号をサポートし、ECDSA 証明書を使用します。

以下は、SIP が (トランスポート層セキュリティ) TLS 接続を行うシナリオです。

- SIP が TLS サーバーとして機能する場合：Unified Communications Manager の SIP トランクインタフェースが、セキュアな SIP 接続の着信に対して TLS サーバーとして機能する場合、SIP トランクインタフェースは、CallManager-ECDSA 証明書がディスク上に存在しているかどうかを判断します。 証明書がディスク上に存在する場合、選択された暗号スイートが **TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256** または **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384** であれば、SIP トランクインターフェイスは CallManager-ECDSA 証明書を使用します。 SIP トランク インターフェイスは、ECDSA 暗号スイートをサポートしないクライアントからの接続に対して、RSA TLS 暗号スイートを引き続きサポートします。 **[TLS 暗号（TLS Ciphers）]** ドロップダウンリストには、Unified Communications Manager が TLS サーバーとして動作したときにサポートされる暗号スイートの設定を許可するオプションが含まれています。
- SIP が TLS クライアントとして機能する場合：SIP トランクインターフェイスが TLS クライアントとして機能する場合、SIP トランクインターフェイスは、**[TLS 暗号（TLS Ciphers）]** フィールドに基づいて、リクエストされた暗号スイートのリストをサーバーに送信します（これには Cisco Unified Communications Manager の **[エンタープライズ パラメータ（Enterprise Parameters）]** ウィンドウにある **[ECDSA 暗号（ECDSA ciphers）]** オプションも含まれます）。 **TLS 暗号**。 この設定により、TLS クライアント暗号スイートリストとサポートされている暗号スイートが優先順位に従って決定されます。

（注） ECDSA クライアント証明書をサポートしていない Unified Communications Manager の以前のリリースで TLS 接続を確立する場合、接続では RSA 暗号スイートが使用されます。 TLS 接続で送信されるクライアント証明書は、選択した TLS 暗号にバインドされません。 Unified Communications Manager の以前のリリースでは、TLS サーバが ECDSA クライアント証明書を受信して処理することもサポートしています。

Unified Communications Manager に接続するために ECDSA 暗号を使用するデバイスは、Identity Trust List (ITL) ファイルに CallManager-ECDSA 証明書が含まれている必要があります。 次に、デバイスは、CallManager-ECDSA 証明書によって保護されている接続を信頼するために、CallManager-ECDSA 証明書をローカル証明書ストアに組み込む必要があります。

CAPF ECDSA サポート

認証局プロキシ機能（CAPF）は、Cisco エンドポイントと Unified Communications Manager の間で証明書を交換するための Cisco 独自の方法です。 Cisco エンドポイントのみが CAPF を使用します。 共通の基準要件を満たすために、CAPF が CAPF バージョン 3 に更新され、ECDSA ローカルで有効な証明書（LSC）がクライントに提供されるようになりました。 顧客が LSC をローカルに作成します。 LSC は、製造元がインストールした証明書（MIC）の代替品です。

CAPF バージョン 3 を使用して、Unified Communications Manager サーバーが電話、CTI アプリケーション、および Jabber クライアントが EC キーを生成するように指示します。 EC キーが生成されると、 Unified Communications Manager は ECDSA LSC を生成して Cisco エンドポイントに送信するか、ECDSA CSR を生成します。

エンドポイントが CAPF バージョン 3 に対応していない場合、Cisco Unified CM Administration の **[電話機の設定（Phone Configuration）]** ウィンドウで、必要な EC キーサイズと RSA キーサイズを設定し、**[EC キー優先、RSA バックアップ（EC Key Preferred, RSA Backup）]** オプションをバックアップとして選択できます。 このバックアップオプションは、CAPF サーバーが EC キーペアにリクエストを送信しようとし、電話が EC キーをサポートしていないとサーバーに通知すると、サーバーは EC キーペアの代わりに RSA キーペアを生成するリクエストを送信します。

（注） Cisco エンドポイントが CAPF バージョン 3 をサポートしていて、**[エンドポイント高度暗号化アルゴリズムサポート（Endpoint Advanced Encryption Algorithm Support）]** パラメータを有効にすることなく **[電話機の設定（Phone Configuration）]** で **[EC 優先、RSA バックアップ（EC Preferred, RSA Backup）]** オプションを選択した場合、ECDSA または RSA ベースの LSC は発行されません。 Cisco エンドポイントが CAPF バージョン 3 をサポートしていない場合、[**エンドポイントの高度暗号化アルゴリズムのサポート**] パラメータを有効または無効にすると、RSA ベースの LSC が発行されます。

（注） [**エンドポイントでの高度な暗号化アルゴリズムのサポート**]パラメータは、電話機が高度TLS暗号を使用してTFTP構成ファイルをダウンロードすることを示します。デフォルトでは、EC暗号が最高の優先順位を持っています。 このソリューションは、MRA なしのオンプレミス展開でのみサポートされています。

エントロピー

強力な暗号化を行うには、エントロピーの堅牢なソースが必要です。エントロピーはデータのランダム性の測定であり、共通の基準要件の最小しきい値を決定するのに役立ちます。暗号化やデータ変換などのデータ変換技術は、その有効性をエントロピーの良いソースに依存しています。 ECDSA などの強力な暗号化アルゴリズムが弱いソースのエントロピーを使用する場合、暗号化は簡単に破られます。

Unified Communications Manager リリース 11.0 では、 Unified Communications Manager のエントロピーソースが改善されています。 エントロピー モニタリング デーモンは、構成を必要としない組み込み機能です。 ただし、 Unified Communications Manager CLI を使ってオフにできます。

以下の CLI コマンドを使って エントロピー監視デーモン サービスを制御します。

CLI コマンド	説明
utils service start Entropy Monitoring Daemon	エントロピー監視デーモン サービスを開始します。
utils service stop Entropy Monitoring Daemon	エントロピー監視デーモン サービスを停止します。
utils service active Entropy Monitoring Daemon	エントロピー監視デーモン サービスを有効にします。これによりさらにカーネルモジュールがロードされます。
utils service deactive Entropy Monitoring Daemon	エントロピー監視デーモン サービスを無効にします。これによりさらにカーネルモジュールがアンロードされます。

HTTPS サポートの設定ダウンロード

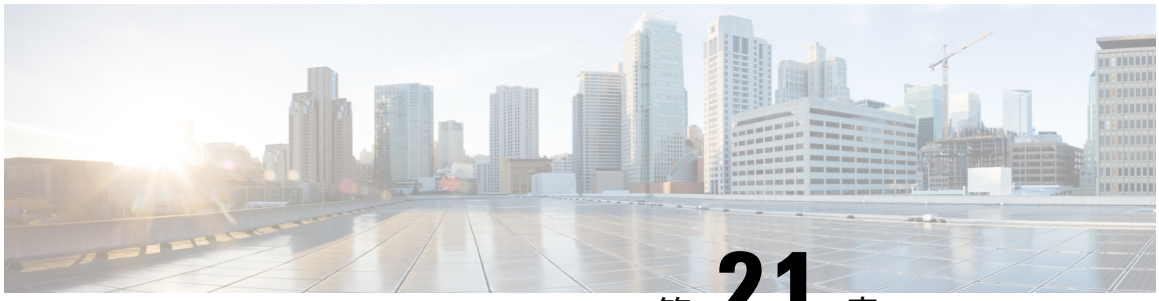
セキュアな設定のダウンロードのために、Unified Communications Manager リリース 11.0 では、以前のリリースで使用されていた HTTP および TFTP インターフェースに加えて、HTTPS をサポートするよう強化されています。 必要に応じて、クライアントとサーバの両方が相互認証を使用します。 ECDSA LSC および暗号化 TFTP 構成で登録されているクライアントは、LSC を提示する必要があります。

HTTPS インターフェイスは、CallManager および CallManager-ECDSA 証明書の両方をサーバ証明書として使用します。

（注） CallManager、CallManager ECDSA、または Tomcat の証明書を更新する場合、TFTP サービスをいったん無効化してから、再度有効化する必要があります。 ポート 6971 は、CallManager および CallManager-ECDSA 証明書の認証に使用され、ポート 6972 は、Tomcat 証明書の認証に使用されます。

CTI マネージャサポート

コンピュータ テレフォニー インテグレーション（CTI）インターフェイスが強化され、4 つの新しい暗号をサポートするようになりました。 暗号スイートは次のとおりです。
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256、
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384、
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 および
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 です。 これらの暗号スイートをサポートすることで、CTI Manager インターフェイスは、Unified Communications Manager に証明書が存在する場合、**CallManager-ECDSA** 証明書を持つ必要があります。 SIP インターフェースと同様に、Unified Communications Manager のエンタープライズパラメータ **[TLS 暗号（TLS Ciphers）]** オプションは、CTI マネージャのセキュアなインターフェイスでサポートされている TLS 暗号を設定するために使用されます。



第 21 章

V.150 の最小必須要件

- V.150 の概要 （287 ページ）
- V.150 タスク フローを設定する （287 ページ）

V.150 の概要

V.150 Minimum Essential Requirements 機能を使用すると、IP ネットワーク経由でモデムで安全な通話を行うことができます。 この機能では、ダイヤルアップモデムを使用して、従来の公衆交換電話網(PSTN)上で動作するモデムとテレフォニーデバイスを大規模に設置します。 V.150.1 勧告は特に、PSTN 上のモデムおよびテレフォニーデバイスからのデータをモデム経由で IP ネットワークとの間でリレーする方法を定義しています。 V.150.1 は、ダイアルアップモデムコールをサポートする IP ネットワーク上のモデムを使用するための ITU-T 勧告です。

Cisco V.150.1 の最小必須要件機能は、国家安全保障局 (NSA) SCIP-216 V.150.1 推奨の最小必須要件 (MER) の要件に準拠しています。 SCIP-216 の推奨により、既存の V.150.1 要件が簡素化されました。

Cisco V.150.1 MER 機能は以下のインターフェイスをサポートします。

- Media Gateway Control Protocol (MGCP) T1(PRI および CAS) および E1(PRI) トランク
- Session Initiation Protocol (SIP) トランク
- アナログ ゲートウェイ エンドポイント用の Skinny Client Control Protocol (SCCP)
- Secure Communication Interoperability Protocol-End Instruments (SCIP-EI)

V.150 タスク フローを設定する

これらのタスクを完了して Unified Communications Manager に V.150 サポートを追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	メディア リソース グループのタスク フローを設定する（289ページ）を行うには、次のサブタスクを実行します。 • 非 V.150 エンドポイントのメディア リソース グループを設定する（290 ページ） • 非 V.150 エンドポイントのメディア リソース グループ リストを設定する（290 ページ） • V.150 エンドポイントのメディア リソース グループを設定する（291 ページ） • V.150 エンドポイントのメディア リソース グループ リストを設定する（291 ページ）	V.150 および非 V.150 デバイスの Media Resource Group と Media Resource Group List を追加します。
ステップ 2	Cisco ゲートウェイ V.150 (MER) を設定する（292 ページ）	V.150 機能をゲートウェイに追加します。
ステップ 3	V.150 MGCP ゲートウェイ ポート インターフェイスを設定します（293 ページ）	MGCP ゲートウェイで V.150 サポートを使用する場合、ポート インターフェイスに V.150 サポートを追加します。
ステップ 4	V.150 SCCP ゲートウェイ ポート インターフェイスを設定する（293ページ）	SCCP ゲートウェイで V.150 サポートを使用する場合、ポート インターフェイスに V.150 サポートを追加します。
ステップ 5	電話の V.150 サポートを設定する（294 ページ）	V.150 コールを発信する電話に V.150 サポートを追加します。
ステップ 6	SIP トランクの設定タスク フロー（295 ページ）を行うには、次のサブタスクのいずれかまたは両方を実行します。 • V.150 の SIP プロファイルの設定（296 ページ） • クラスター全体の V.150 フィルターを設定する（296 ページ） • V.150 フィルタを SIP トランク セキュリティ プロファイルに追加（297 ページ）	V.150 通話に使用される SIP トランクに V.150 サポートを追加します。

	コマンドまたはアクション	目的
	• V.150 の SIP トランクを設定する（297 ページ）	
ステップ 7	V.150 MER 機能を使用するには、この機能をサポートするためにゲートウェイで IOS を設定する必要があります。	IOS ゲートウェイ構成設定の詳細については、『http://www.cisco.com/c/en/us/td/docs/ios/12_4t/12_4t4/mer_cg_15_1_4M.html』を参照してください。

メディア リソース グループのタスク フローを設定する

システムには、基本的なコールコントロール機能がセットアップ済みである必要があります。通話コントロールシステムのセットアップ方法については、『Cisco Unified Communications Manager システム設定ガイド』を参照してください。

Unified Communications Managerには、次のいずれかのリリースがインストールされている必要があります:

- 最小バージョンは Release 10.5 (2) SU3 です
- 11.0 の場合、最小バージョンは 11.0(1)SU2 になります。
- 11.5 (1) 以降のすべてのリリースでこの機能がサポートされます
- *Cisco IOS* リリース 15.6(2)T 以降が必要です。

V.150 はメディア ターミネーション ポイント (MTP) ではサポートされていません。 V.150 コールを処理するデバイス、トランク、およびゲートウェイから MTP を削除することを推奨します。

次のタスクを完了して、2 セットのメディアリソースグループ（非 V.150 コール用の MTP リソースを持つメディアリソースグループと、V.150 コール用の MTP リソースを持たないメディアリソースグループ）を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	非 V.150 エンドポイントのメディア リソース グループを設定する （290 ページ）	非 V.150 エンドポイントに対して、MTP でメディア リソース グループを設定できます。
ステップ 2	非 V.150 エンドポイントのメディア リソース グループ リストを設定する （290 ページ）	非 V.150 エンドポイント用の MTP メディア リソースを含むメディア リソース グループ リストを構成します。

	コマンドまたはアクション	目的
ステップ 3	V.150 エンドポイントのメディア リソース グループを設定する （291 ページ）	セキュアな V.150 コールのために、MTP リソースなしのメディアリソースグループを設定します。
ステップ 4	V.150 エンドポイントのメディア リソース グループ リストを設定する （291 ページ）	セキュアな V.150 エンドポイントのメディアリソースグループに必要なリソースを追加した後、MTP を含まないメディア リソース グループ リストを設定します。

非 V.150 エンドポイントのメディア リソース グループを設定する

この手順を使用して、非 V.150 エンドポイントの MTP リソースを含む新しいメディアリソースグループを追加します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから [**メディアリソース** > **]** > **[メディアリソースグループ]** を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [**名前**] フィールドでメディアリソースグループ名を入力し、[**V.150 端末では使用しない**] とします。

ステップ 4 **利用可能なメディアリソース** フィールドから MTP 端末のみを選択して、 **下向き矢印アイコン** をクリックします。
選択した端末が、 **選択したメディアリソース** フィールドに表示されます。

ステップ 5 **[保存（Save）]** をクリックします。

非 V.150 エンドポイントのメディア リソース グループ リストを設定する

非 V.150 エンドポイントのメディア リソース グループを設定する （290 ページ）

この手順を使用して、非V.150エンドポイント用のMTPリソースを持つ新しいメディアリソースグループリストを追加します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから **[メディアリソース]** > **Media Resource Group List**を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 [名前] フィールドにメディアリソースグループリストの名前を 非 **V.150** として入力します。

ステップ 4 **[使用可能なメディアリソース（Available Media Resources）]** フィールドで、**[V.150 デバイス用（For V.150 Devices）]** という名称の V.150 MER リソースグループを選択し、**下矢印キー**をクリックします。
選択した端末が、 **選択したメディアリソース** フィールドに表示されます。

ステップ 5 **[保存（Save）]** をクリックします。

V.150 エンドポイントのメディア リソース グループを設定する

この手順を使用して、V.150 デバイス用の新しいメディアリソースグループを追加します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから [**メディアリソース** > **]** > **[メディアリソースグループ] を選択します。**

ステップ 2 [新規追加] をクリックします。

ステップ 3 [**名前**] フィールドでメディアリソースグループ名を入力し、[**V.150 端末では使用しない**] とします。

ステップ 4 **利用可能なメディアリソース** フィールドから、複数のデバイスを選択し、**下矢印キー**をクリックします。MTP リソースは除外してください。
選択した端末が、 **選択したメディアリソース** フィールドに表示されます。

ステップ 5 **[保存（Save）]** をクリックします。

V.150 エンドポイントのメディア リソース グループ リストを設定する

V.150 エンドポイントのメディア リソース グループを設定する （291 ページ）

この手順を使用して、V.150 デバイス用に MTP リソースなしのメディアリソースグループリストを追加します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから **[メディアリソース]** > **[メディアリソースグループリスト]**を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **[名前（Name）]** フィールドにメディア リソース グループ リストの名前を **[V.150]** として入力します。

ステップ 4 **[使用可能なメディアリソース（Available Media Resources）]** フィールドで、**[V.150 デバイス用（For V.150 Devices）]** という名称の V.150 MER リソースグループを選択し、**下矢印キー**をクリックします。
選択したメディアリソースグループが、 **選択したメディアリソース** フィールドに表示されます。

ステップ 5 **[保存（Save）]** をクリックします。

Cisco ゲートウェイ V.150 (MER) を設定する

この手順を使ってゲートウェイを Cisco V.150 (MER) 用に設定します。

手順

ステップ 1 Cisco Unified Communications Manager Administration から、**[デバイス（Device）]** > **[ゲートウェイ（Gateway）]**を選択します。

ステップ 2 [新規追加] をクリックします。

ステップ 3 **ゲートウェイタイプ** ドロップダウンリストからゲートウェイを選択します。

ステップ 4 [次へ（Next）]をクリックします。

ステップ 5 [**プロトコル** ドロップダウン リストから、プロトコルを選択します。

ステップ 6 ゲートウェイに選択したプロトコルに応じて、以下を実行します。

- MGCP の場合、 **ドメイン名** フィールドに、ゲートウェイで設定されているドメイン名を入力します。
- SCCP の場合、 **MAC アドレス(最後の 10 文字)** フィールドに、ゲートウェイの MAC アドレスを入力します。

ステップ 7 **[Unified Communications Manager グループ（Unified Communications Manager Group）]** ドロップダウンリストから、**[デフォルト（Default）]** を選択します。

ステップ 8 [設定済みのスロット、VIC、およびエンドポイント（Configured Slots、VICs and Endpoints）] 領域で次の手順を実行します。

a) 各 [モジュール（Module）] ドロップダウン リストで、ゲートウェイにインストールされているネットワーク インターフェイス モジュール ハードウェアに対応するスロットを選択します。

b) 各 [サブユニット（Subunit）] ドロップダウン リストで、ゲートウェイにインストールされている VIC を選択します。

c) **[保存（Save）]** をクリックします。
ポートアイコン が表示されます。 各 **ポートアイコン** がゲートウェイの利用可能な **ポートインターフェース** に対応しています。 **ポートインターフェイス**を設定するには、該当する**ポートのアイコン**をクリックします。

ステップ 9 [ゲートウェイの設定（Gateway Configuration）]ウィンドウでその他のフィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 10 **[保存（Save）]** をクリックします。

V.150 MGCP ゲートウェイ ポート インターフェイスを設定します

この手順を使用して V.150 MGCP ゲートウェイ ポート インターフェイスを設定します。

手順

ステップ 1 Cisco Unified Communications Manager Administration から、**[デバイス（Device）]** > **[ゲートウェイ（Gateway）]** を選択します。

ステップ 2 既存のゲートウェイの設定を変更するための適切な検索基準を入力して、**[検索（Find）]** をクリックします。

ステップ 3 **Configured Slots, VICs, and Endpoints** エリアで、V.150 MER 用のポートを設定するモジュールとサブユニットを見つけ、対応する **ポートアイコン**をクリックします。

ステップ 4 **Device Protocol** ドロップダウンリストから、 **Digital Access T1** または **Digital Access PRI** を選択し、[**次へ**] をクリックします。

（注）
デバイスプロトコル ドロップダウンリストは、 **Configured Slots, VICs, and Endpoints** エリアでT1ポートが選択された場合にのみ表示されます。

ゲートウェイ構成 ウィンドウに、ポートのインターフェース構成が表示されるようになりました。

ステップ 5 **Media Resource Group List** named **V.150** を選択します。

ステップ 6 **V150 (サブセット)** チェックボックスを選択します。

ステップ 7 必要に応じて残りのフィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 8 **[保存（Save）]** をクリックします。

ステップ 9 （任意） ゲートウェイに追加のポート インターフェースを設定する場合は、[**関連リンク**] ドロップダウンリストから **[MGCP 設定に戻る]** を選択します。 **[実行]** をクリックします。 別のポートインタフェースを選択することができます。

V.150 SCCP ゲートウェイ ポート インターフェイスを設定する

この手順で V.150 SCCP ゲートウェイ ポート インターフェイスを設定します。

手順

ステップ 1 Cisco Unified Communications Manager Administration から、**[デバイス（Device）]** > **[ゲートウェイ（Gateway）]** を選択します。

ステップ 2 既存のゲートウェイの設定を変更するための適切な検索基準を入力して、**[検索（Find）]** をクリックします。

ステップ 3 **Configured Slots, VICs, and Endpoints** エリアで、V.150 MER 用のポートを設定するモジュールとサブユニットを見つけ、対応する **ポートアイコン**をクリックします。

ステップ 4 **メディアリソースグループリスト**「**V.150**」 を選択します。

ステップ 5 **[製品固有の設定レイアウト（Product Specific Configuration Layout）]** 領域で、**[潜在機能登録設定（Latent Capability Registration Setting）]** ドロップダウンメニューが表示されたら、**[モデムリレー（Modem Relay）]** または **[モデムリレーとパススルー（Modem Relay and Passthrough）]** から選択します。

ステップ 6 必要に応じて残りのフィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 7 **[保存（Save）]** をクリックします。

電話の V.150 サポートを設定する

この手順で電話に V.150 サポートを追加します。 次の電話タイプは V.150 をサポートします。

- Cisco 7962—Cisco 7962 として登録されたサードパーティ SCCP エンドポイント
- Cisco 7961G-GE—Cisco 7961G-GE として登録されているサードパーティ SCCP エンドポイント
- サードパーティ AS-SIP エンドポイント

手順

ステップ 1 必須: 目的の電話番号と同じユーザ ID を持つエンドユーザを作成します。

ステップ 2 必須: サードパーティ AS-SIP SIP エンドポイント用に、エンドユーザ設定ウィンドウのダイジェスト認証フィールドを設定します。

新規エンドユーザの構成方法の詳細は、「エンドユーザを手動でプロビジョニングする」の章を参照してください。 「」Cisco Unified Communications Manager システム設定ガイド

ステップ 3 Cisco Unified Communications Manager Administrationから **端末** > **電話**を選択します。

ステップ 4 次のいずれかの手順を実行します。

- 既存の電話に V.150 を設定するには、[**検索**] をクリックして電話を選択します。

- V.150 用に新しい電話を設定するには、[**新規追加**] をクリックします。

ステップ 5 **電話タイプ** ドロップダウンリストから、V.150 をサポートする電話タイプを 1 つ選択し、[**次へ**] をクリックします。

ステップ 6 Cisco 7962 として登録されているサードパーティの SCCP エンドポイントの場合、[**Device Protocol**] ドロップダウンリストから **SCCP** を選択し、[**次へ**] をクリックします。

ステップ 7 **メディアリソースグループリスト** ドロップダウンメニューから **V.150**を選択します。

ステップ 8 サードパーティ AS-SIP SIP エンドポイントのみ、以下のフィールドを設定します。

- **ダイジェストユーザの** ドロップダウンから、この電話のエンドユーザを選択します。 エンドユーザはダイジェスト認証に使用されます。
- **メディア終端点が必要な** チェックボックスはチェックを外しておきます。
- **音声通話とビデオ通話の早期オファーのサポート** チェックボックスを選択します。

ステップ 9 **[保存（Save）]** をクリックします。

ステップ 10 **[設定の適用（Apply Config）]** をクリックします。

ステップ 11 **OK**をクリックします。

SIP トランクの設定タスク フロー

この手順を使用して SIP トランクタスクフローを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	V.150 の SIP プロファイルの設定 （296 ページ）	SIP トランクの SIP ベスト エフォート アーリー オファー サポートを含む SIP プロファイルを設定します。
ステップ 2	クラスター全体の V.150 フィルターを設定する （296 ページ）	これはオプションです。 SIP V.150 SDP オファー フィルタリングのクラスタ全体のデフォルト設定を構成します。
ステップ 3	V.150 フィルタを SIP トランク セキュリティ プロファイルに追加 （297 ページ）	特定の SIP トランクに指定できる SIP トランク セキュリティ プロファイル内に V.150 フィルタを設定します。
ステップ 4	V.150 の SIP トランクを設定する （297 ページ）	V.150 コールを処理する SIP トランクの V.150 サポートを構成します。

V.150 の SIP プロファイルの設定

この手順を使用して、SIP トランクの SIP ベストエフォートアーリーオファーサポートを持つ SIP プロファイルを設定します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationで **端末** > **端末設定** > **SIP プロファイル** を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[新規追加] をクリックします。
- 既存のプロファイルを選択するには、[**検索**] をクリックして、SIP プロファイルを選択します。

ステップ 3 [**名前**] フィールドに、V.150 の SIP 名を入力します。

ステップ 4 [説明（Description）]フィールドに、トランクの説明を入力します。

ステップ 5 [**Early Offer Support for Voice and video class**] ドロップダウンリストから [**] [ベストエフォートを選択 (MTP 挿入なし)]** を選択します。

ステップ 6 必要に応じてその他の構成を入力します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 7 **[保存（Save）]** をクリックします。

クラスター全体の V.150 フィルターを設定する

この手順を使用して、SIP V.150 SDP オファーフィルタリングのクラスタ全体のデフォルト設定を構成します。

（注） クラスタ全体のサービスパラメータ設定とは異なる **SIP V.150 SDP オファイルタリング** 値を SIP トランクセキュリティプロファイル内に設定した場合、そのセキュリティプロファイルを使用するトランクについては、セキュリティプロファイルの設定がクラスタ全体のサービスパラメータ設定を上書きします。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから **システム** > **サービスパラメータを選択します**。

ステップ 2 **サーバ** ドロップダウンリストから、アクティブなサーバを選択します。

ステップ 3 [サービス（Service）] ドロップダウン リストから、[Cisco CallManager] を選択します。

ステップ 4 **クラスター全体のパラメータ (デバイス- SIP)** セクションで **SIP V.150 SDP オファーフィルタリング** の値を設定します。

ステップ 5 ドロップダウンリストから **SIP V.150 SDP オファーフィルタリング** を選択します。

ステップ 6 希望するフィルタリングアクションを指定します。

ステップ 7 **[保存（Save）]** をクリックします。

V.150 フィルタを SIP トランク セキュリティ プロファイルに追加

この手順を使用して、SIP トランクセキュリティプロファイル内で V.150 フィルタを指定します。

（注） クラスタ全体のサービスパラメータ設定とは異なる **SIP V.150 SDP オファイルタリング** 値を SIP トランクセキュリティプロファイル内に設定した場合、そのセキュリティプロファイルを使用するトランクについては、セキュリティプロファイルの設定がクラスタ全体のサービスパラメータ設定を上書きします。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから **システム** > **セキュリティ** > **SIP トランクセキュリティプロファイル**を選択します。

ステップ 2 次のいずれかの作業を実行します。

- 検索基準を入力し、**[検索]** をクリックしてリストから既存のプロファイルを選択し、既存の SIP トランクセキュリティプロファイルの設定を変更します。
- **新規追加** をクリックして新しい SIP トランクセキュリティプロファイルを追加します。

ステップ 3 [**SIP V.150 アウトバウンド SDP オファー フィルタリング**] ドロップダウンリストの値を設定します。

（注）
デフォルト設定では、 **SIP V.150 アウトバウンド SDP フィルタリング オファー** クラスタ全体のサービスパラメータの値が使用されます。

ステップ 4 **SIP トランクセキュリティプロファイルの構成** ウィンドウの残りのフィールドを構成します。フィールドとその設定オプションの詳細については、オンラインヘルプを参照してください。

ステップ 5 **[保存（Save）]** をクリックします。

V.150 の SIP トランクを設定する

この手順を使用して、SIP トランクの設定を構成します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから、 **端末** > **トランク**を選択します。

ステップ 2 次のいずれかの手順を実行します。

- 新しいプロファイルを作成するには、[新規追加] をクリックします。
- [**検索**] をクリックして、既存のSIPトランクを選択します。

ステップ 3 新しいトランクの場合、以下を実行します。

- [トランクタイプ（Trunk Type）]ドロップダウン リストから [SIPトランク（SIP Trunk）]を選択します。
- **プロトコルタイプ** ドロップダウンリストから **SIP を選択します**。
- **トランクサービスタイプ** ドロップダウンリストから、 **なし(デフォルト) を選択します**。
- [次へ（Next）]をクリックします。

ステップ 4 **名前** フィールドに SIP トランク名を入力します。

ステップ 5 **説明** フィールドに SIP トランクの説明を入力します。

ステップ 6 [**メディアリソースグループリスト**] ドロップダウンリストから、「V.150」 という名前のメディアリソースグループリストを選択します。

ステップ 7 SIP トランクの宛先アドレスを設定します。

a) [宛先アドレス（Destination Address）]テキスト ボックスに、トランクに接続するサーバまたはエンドポイントの IPv4 アドレス、完全修飾ドメイン名、または DNS SRV レコードを入力します。

b) 宛先が DNS SRV レコードの場合は、[宛先アドレスはSRV（Destination Address is an SRV）] チェック ボックスをオンにします。

c) 接続先を追加するには、**[+]** をクリックします。 SIP トランクの宛先を最大 16 個まで追加できます。

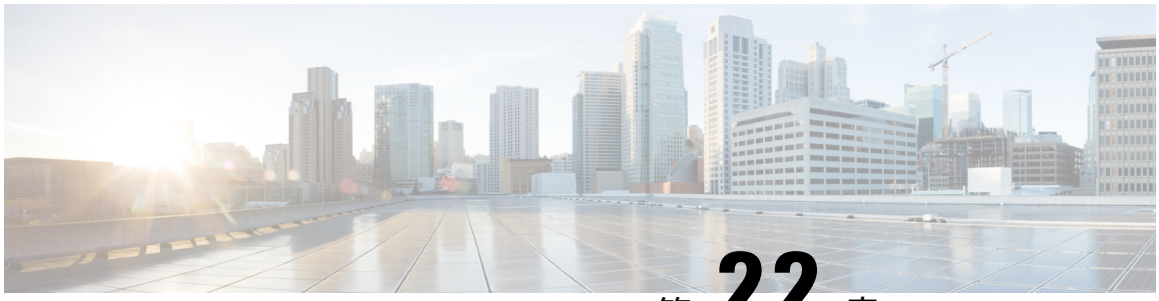
ステップ 8 ドロップダウン リストから、**「SIP トランク セキュリティ プロファイル」**の手順で作成した SIP トランク セキュリティ プロファイルの名前を選択します。

ステップ 9 **[SIP プロファイル]** ドロップダウンリストから、[ベストエフォートのアーリーオファー] 設定でセットアップした SIP プロファイルを指定します。

ステップ 10 **メディア終端点が必要な** チェックボックスはチェックを外しておきます。

ステップ 11 [Trunk Configuration]ウィンドウのその他のフィールドを設定します。 フィールドとその設定オプションの詳細については、オンライン ヘルプを参照してください。

ステップ 12 **[保存（Save）]** をクリックします。



第 22 章

IPSec のセットアップ

• IPSec の概要 （299 ページ）

IPSec の概要

IPsec は、暗号セキュリティ サービスを使用した IP ネットワーク経由の非公開でセキュアな通信を保証するフレームワークです。 IPsec ポリシーが IPsec セキュリティ サービスの設定に使用されます。 このポリシーは、ネットワーク上のほとんどのトラフィック タイプにさまざまなレベルの保護を提供します。 コンピュータ、部門（OU）、ドメイン、サイト、またはグローバル企業のセキュリティ要件を満たすように IPsec ポリシーを設定できます。

ネットワークインフラストラクチャ内での IPsec のセットアップ

このセクションでは、IPsec の設定方法については説明しません。 代わりに、ネットワーク インフラストラクチャで IPsec を構成するための考慮事項と推奨事項を提供します。 Unified Communications Manager とデバイス間ではなく、ネットワークインフラストラクチャに IPsec を設定する場合は、IPsec を設定する前に次の情報を確認してください。

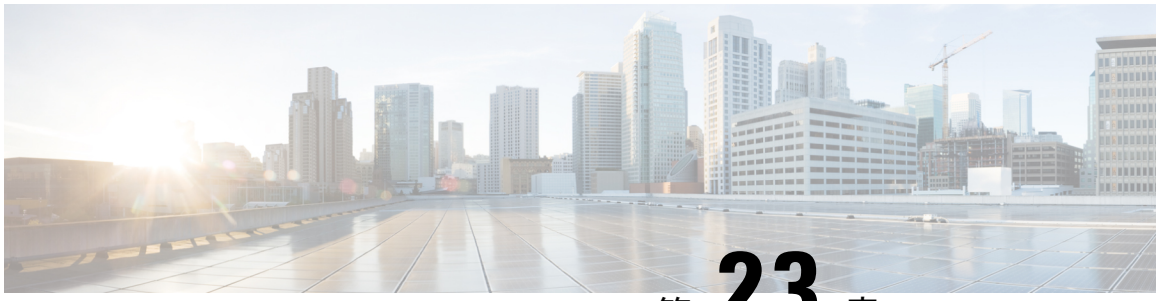
- IPsec を Unified Communications Manager 自体ではなく、インフラストラクチャにプロビジョニングすることをお勧めします。
- IPsec を設定する前に、既存の IPsec または VPN 接続、プラットフォーム CPU への影響、帯域幅への影響、ジッターまたは遅延、およびその他のパフォーマンスメトリックを考慮してください。
- 音声およびビデオ対応 *IPsec* 仮想プライベートネットワークソリューションリファレンスネットワーク設計ガイドを確認してください。
- 『*CiscoIOS* セキュリティ設定ガイド、リリース *12.2*』（以降）を確認してください。
- セキュアな CiscoIOS MGCP ゲートウェイで IPsec 接続のリモート エンドを終了します。
- テレフォニーサーバーが存在するネットワークの信頼できる範囲内のネットワークデバイスでホスト側を終了します。例えば、ファイアウォール、アクセスコントロールリスト（ACL）、または他のレイヤー 3 デバイスの背後などです。

- 主催者側の IPsec 接続を終端するために使用する機器は、ゲートウェイの数とそれらのゲートウェイへの予想されるコール量に応じて決まります。例えば、Cisco VPN 3000 シリーズコンセントレータ、Catalyst 6500 IPsec VPN サービスモジュール、または Cisco サービス統合型ルーターを使用できます。
- セキュアゲートウェイとトランクの設定に関するトピックで指定されている順番に手順を実行してください。

注意 IPsec 接続を設定しなかったり、接続がアクティブであることを確認しなかったりすると、メディアストリームのプライバシーが侵害される可能性があります。

Unified Communications Manager とゲートウェイまたはトランク間の IPsec セットアップの構成と管理

Unified Communications Manager と記載されているゲートウェイまたはトランクとの間の IPSec の設定については、『Cisco Unified Communications Manager アドミニストレーション ガイド』の「IPSec ポリシーの管理」の章を参照してください。



第 23 章

CTI、JTAPI、および TAPI の認証と暗号化のセットアップ

この章では、CTI、JTAPI、および TAPI アプリケーションを保護する方法について簡単に説明します。 また、CTI/TAPI/JTAPI アプリケーションの認証と暗号化を設定するために、Unified Communications Manager Administration で行う必要がある作業についても説明しています。

このドキュメントでは、Unified Communications Manager Administration で利用可能な CiscoJTAPI または TSP プラグインのインストール方法、またはインストール中のセキュリティパラメータの設定方法については説明していません。 同様に、このドキュメントでは、CTI 制御デバイスまたは回線の制限を設定する方法については説明していません。

- CTI、JTAPI、および TAPI アプリケーションの認証 （301 ページ）
- CTI、JTAPI、および TAPI アプリケーションの暗号化 （303 ページ）
- CTI、JTAPI、および TAPI アプリケーションの CAPF 関数 （305 ページ）
- CTI、JTAPI、および TAPI の保護 （312 ページ）
- アプリケーション ユーザとエンド ユーザをセキュリティ関連のアクセス コントロール グループに追加する （314 ページ）
- JTAPI/TAPI セキュリティ関連のサービスパラメータのセットアップ （315 ページ）
- アプリケーションまたはエンドユーザの証明書操作状況を表示する （316 ページ）

CTI、JTAPI、および TAPI アプリケーションの認証

Unified Communications Manager により、CTIManager と CTI/JTAPI/TAPI アプリケーション間のシグナリング接続とメディアストリームをセキュアにすることができます。

（注） CiscoJTAPI/TSP プラグインのインストール時にセキュリティ設定を構成したものと想定されます。 また、Cisco CTL クライアントまたは CLI コマンド set **utils ctl で設定されているように、クラスターセキュリティモードは混合モードと等しいと想定します**。 本章で説明されているタスクを実行する際にこれらの設定が構成されていない場合、CTIManager とアプリケーションは非セキュアなポート、ポート 2748 経由で接続します。

CTIManager とアプリケーションは、相互に認証された TLS ハンドシェイク (証明書交換) を通じて、相手の身元を確認します。 TLS 接続が確立されると、CTIManager とアプリケーションは TLS ポートのポート 2749 経由で QBE メッセージを交換します。

アプリケーションの認証を行うために、CTIManager は Unified Communications Manager 証明書を使用します。この証明書には、インストール時に Unified Communications Manager サーバに自動的にインストールされる自己署名証明書、またはサードパーティの CA 署名証明書が使用されます。

CLI コマンド set **utils ctl** または Cisco CTL クライアントで CTL ファイルを生成すると、この証明書が自動的に CTL ファイルに追加されます。 アプリケーションは CTIManager への接続を試みる前に、TFTP サーバから CTL ファイルをダウンロードします。

JTAPI/TSP クライアントが初めて CTL ファイルを TFTP サーバからダウンロードするとき、JTAPI/TSP クライアントは CTL ファイルを信頼します。 JTAPI/TSP クライアントは CTL ファイルを検証しないため、ダウンロードは安全な環境で行うことを推奨します。JTAPI/TSP クライアントは、後続の CTL ファイルのダウンロードを確認します。たとえば、CTL ファイルを更新した後、JTAPI/TSP クライアントは CTL ファイルのセキュリティトークンを使用して、ダウンロードする新しい CTL ファイルのデジタル署名を認証します。 このファイルの内容には Unified Communications Manager 証明書および CAPF サーバ証明書が含まれます。

CTL ファイルが危険にさらされている場合、JTAPI/TSP クライアントはダウンロードされた CTL ファイルを置き換えません。クライアントはエラーをログに記録し、既存の CTL ファイル中の古い証明書を使用して TLS 接続の確立を試みます。 CTL ファイルが変更されているか、または不正使用されている場合、接続は失敗する可能性があります。 CTL ファイルのダウンロードが失敗し、しかも複数の TFTP サーバが存在する場合、ファイルをダウンロードするように別の TFTP サーバを設定できます。 JTAPI/TAPI クライアントは、次の状況ではどのポートにも接続しません。

- 何らかの理由でクライアントが CTL ファイルをダウンロードできません。たとえば、CTL ファイルが存在しません。
- クライアントに既存の CTL ファイルがありません。
- アプリケーションユーザをセキュアな CTI ユーザとして構成しました。

CTIManager で認証するために、アプリケーションは 認証局プロキシ 機能 (CAPF) が発行する証明書を使用します。 アプリケーションと CTIManager 間のすべての接続で TLS を使用するには、アプリケーション PC で実行される各インスタンスに固有の証明書が必要です。 1 つの証明書ですべてのインスタンスをカバーできるわけではありません。 Cisco Unified Communications Manager Assistant サービスが実行されているノードに証明書が確実にインストールされるように、 Cisco Unified Communications Manager Administrationの各アプリケーション・ユーザ CAPF プロファイル構成またはエンドユーザ CAPF プロファイル構成に対して固有のインスタンス ID を構成します。次のように、 「アプリケーションおよびエンドユーザ CAPF プロファイルの構成設定」を参照してください。

ヒント ある PC からアプリケーションをアンインストールして別の PC にインストールする場合、新しい PC の各インスタンスに対して新しい証明書をインストールする必要があります。

Unified Communications Manager でアプリケーションユーザまたはエンドユーザを標準 CTI セキュアコネクションユーザグループに追加し、アプリケーションの TLS を有効にする必要があります。ユーザをこのグループに追加し、証明書をインストールした後、アプリケーションはユーザが TLS ポート経由で接続することを確認します。

CTI、JTAPI、および TAPI アプリケーションの暗号化

ヒント　認証は暗号化の最小要件として機能します。つまり、認証を設定していない場合、暗号化を使用することはできません。

Unified Communications Manager、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしていません。 CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポートしている可能性があります。

アプリケーションと CTIManager の間のメディア ストリームをセキュアにするには、アプリケーションユーザまたはエンドユーザを標準 CTI SRTP キーマテリアルの受信を許可するユーザ グループに追加します Unified Communications Manager。 これらのユーザが標準 CTI セキュア接続ユーザグループにも存在し、クラスタセキュリティモードが混合モードである場合、CTIManager はアプリケーションとの TLS 接続を確立し、メディアイベントでアプリケーションにキーマテリアルを提供します

（注）　クラスタセキュリティモードでは、スタンドアロンサーバまたはクラスタのセキュリティ機能を設定します。

アプリケーションが SRTP キー情報を記録または保存することはありませんが、アプリケーションはキー情報を使用して RTP ストリームを暗号化し、CTIManager からの SRTP ストリームを復号化します。

何らかの理由でアプリケーションがノンセキュア ポートのポート 2748 に接続する場合、CTIManager はキー情報を送信しません。 制限を設定したために、CTI/JTAPI/TAPI がデバイスまたはディレクトリ番号を監視または制御できない場合、CTIManager はキー情報を送信しません。

ヒント　アプリケーションが SRTP セッションキーを受信するには、アプリケーションまたはエンドユーザーが、[標準CTIを有効にする（Standard CTI Enabled）]、[標準CTIセキュア接続（Standard CTI Secure Connection）]、および [標準 CTI SRTP 重要素材の受信許可（Standard CTI Allow Reception of SRTP Key Material）] の 3 つのグループに属している必要があります。

ただし、Unified Communications Manager は CTI ポートとルートポイントとの間の安全なコールを容易にすることができますが、アプリケーションがメディアパラメータを処理するため、安全なコールをサポートするようにアプリケーションを設定する必要があります。

CTI ポート/ルートポイントは、動的または静的な登録によって登録されます。 ポート/ルートポイントが動的登録を使用する場合、メディアパラメータは各コールに対して指定されます。静的登録の場合、メディアパラメータは登録時に指定され、呼び出しごとに変更することはできません。 CTIports/ルートポイントが TLS 接続を介して CTIManager に登録されると、アプリケーションがデバイス登録リクエストで有効な暗号化アルゴリズムを使用し、相手側がセキュアな場合、デバイスは安全に登録され、メディアは SRTP 経由で暗号化されます。

CTI アプリケーションが確立済みの通話の監視を開始するとき、アプリケーションは RTP イベントを受信しません。 確立された通話については、CTI アプリケーションは DeviceSnapshot イベントを提供します。これは、通話のメディアがセキュアか非セキュアかを定義します。このイベントは暗号化キーを提供しません。

CTI ポートのより強力な暗号スイート

CTI ポートが TLS 接続を介して CTI Manager に登録されると、デバイスは安全に登録され、メディアは Secure Real-Time Transport Protocol (SRTP) によって暗号化されます。アプリケーションがデバイス登録リクエストで有効な暗号化アルゴリズムを使用し、相手方が安全である場合。

Unified Communications Manager は、CTI ポート用の Skinny Client Control Protocol (SCCP) インターフェイスでより強力な暗号スイートを提供し、発信側と着信側の間の安全なメディア通知を可能にします。 CTI ポートで SRTP を有効にするために、CTI アプリケーションは暗号強度のサポートされているアルゴリズム ID を提供することで登録します。

Unified Communications Manager は、CTI ポートを含むセキュアなコールで、以下の追加アルゴリズムのネゴシエーションを許可するように強化されました。

- CCM_AES_CM_128_HMAC_SHA1_32 (CiscoMediaEncryptionAlgorithmType.AES_128_COUNTER)
- CCM_AES_CM_128_HMAC_SHA1_80 (CiscoMediaEncryptionAlgorithmType.AES_128_COUNTER)
- CCM_AEAD_AES_128_GCM (CiscoMediaEncryptionAlgorithmType.AEAD_128_COUNTER)
- CCM_AEAD_AES_256_GCM (CiscoMediaEncryptionAlgorithmType.AEAD_256_COUNTER)

電話を受けると、 Unified Communications Manager は CTI アプリケーションで指定されたメディアと暗号化機能をネゴシエートし、着信側の電話との CTI ポートを登録します。 一致するアルゴリズムがある場合、Unified CM はキー情報を両側に送信して、パケットを復号化し、メディアを監視または記録します。

制約事項

Unified Communications Manager は CCM_F8_128_HMAC_SHA1_32 および CCM_F8_128_HMAC_SHA1_80 アルゴリズムをサポートしていません。 CTI アプリケーションがこれらのサポートされていないアルゴリズムでメディアを終端する CTI ポートを登録しようとした場合、Unified CM はそれを無視し、残りのアルゴリズムの中から最適なものを選択します。 システムがこれら 2 つ以外のアルゴリズムで構成されていない場合、Unified CM は既存

の動作に切り替えるのではなく、デフォルトでCCM_AES_CM_128_HMAC_SHA1_32を選択します。

CTI、JTAPI、および TAPI アプリケーションの CAPF 関数

Unified Communications Manager と共に自動的にインストールされる CAPF（認証局プロキシ機能）は、設定に応じて、コンピュータ電話統合/TAPI/TAPIアプリケーションに対して次のタスクを実行します。

- 認証文字列を使って JTAPI/TSP クライアントを認証します。
- ローカルで有効な証明書（LSC）を コンピュータ電話統合/JTAPI/TAPI アプリケーションユーザーまたはエンドユーザーに発行します。
- 既存のローカルで有効な証明書をアップグレードします。
- 表示とトラブルシューティングのために証明書を取得します。

JTAPI/TSPクライアントがCAPFと対話するとき、クライアントは認証文字列を使用してCAPFに対して自身を認証します。それから、クライアントは公開鍵と秘密鍵のペアを生成し、公開鍵を署名されたメッセージでCAPFサーバに転送します。 秘密鍵はクライアント内に残り、外部に公開されることはありません。 CAPFは証明書に署名し、署名したメッセージで証明書をクライアントに送り返します。

アプリケーションユーザまたはエンドユーザに証明書を発行するには、それぞれ [アプリケーションユーザのCAPFプロファイル設定] ウィンドウまたは [エンドユーザのCAPFプロファイル設定] ウィンドウで設定を行います。 以下の情報では、 Unified Communications Manager がサポートする CAPF プロファイル間の違いについて説明しています。

- **アプリケーションユーザCAPFプロファイル**このプロファイルにより、ローカルで有効な証明書を発行してアプリケーションユーザを保護し、CTIManager サービスとアプリケーションの間で TLS 接続を開くことができます。

  1 つのアプリケーション ユーザ CAPF プロファイルが、サーバ上のサービスまたはアプリケーションの単一インスタンスに対応します。 同じサーバ上で複数のウェブ サービスまたはアプリケーションをアクティベートする場合、サーバ上の各サービスに対して 1 つずつ、複数のアプリケーション ユーザ CAPF プロファイルを設定する必要があります。

  クラスタ内の 2 つのサーバでサービスまたはアプリケーションをアクティベートする場合、各サーバに 1 つずつ、合計 2 つのアプリケーション ユーザ CAPF プロファイルを設定する必要があります。

- **エンドユーザCAPFプロファイル**—このプロファイルにより、ローカルで有効な証明書を CTI クライアントに発行し、CTI クライアントが TLS 接続経由で CTIManager サービスと通信できるようになります。

ヒント JTAPI クライアントは、[JTAPI 基本設定] ウィンドウで設定したパスに、LSC を Java キーストア形式で保存します。 TSP クライアントは LSC を暗号化された形式で既定のディレクトリまたは設定したパスに保存します。

以下の情報は、通信障害や電源障害の発生時に適用されます。

- 証明書のインストール中に通信障害が発生すると、JTAPI クライアントは 30 秒間隔でさらに 3 回証明書の取得を試みます。 この値を構成することはできません。

  TSP クライアントの場合、再試行と再試行タイマーを設定できます。TSP クライアントが割り当てられた時間内に証明書の取得を試みる回数を指定することにより、これらの値を設定します。 両方の値のデフォルトは 0 です。1 (1 回のリトライ)、2、または 3 を指定することで、最大 3 回の再試行を設定できます。各再試行の時間は最大30秒まで設定できます。

- JTAPI/TSP クライアントが CAPF でセッションを試みている間に電源障害が発生すると、クライアントは電源が回復した後に証明書のダウンロードを試みます。

CAPF システム インタラクションと CTI、JTAPI、および TAPI アプリケーションの要件

CAPF には以下の要件があります。

- アプリケーションユーザおよびエンドユーザの CAPF プロファイルを設定する前に、**エンタープライズパラメータ設定** ウィンドウのクラスタセキュリティモードが 1 (混合モード) になっていることを確認してください。
- CAPF を使用するには、パブリッシャノードで Cisco 認証局プロキシ機能サービスを有効にする必要があります。
- 同時に多くの証明書を生成すると、コール処理の中断が発生する可能性があるため、スケジュールされたメンテナンス期間中に CAPF を使用することを推奨します。
- 証明書操作の間、パブリッシャノードが機能し、実行中であることを確認してください。
- 証明書操作の間、CTI/JTAPI/TAPI アプリケーションが機能していることを確認してください。

認証局プロキシ 機能 サービスのアクティベーション

Unified Communications Managerで、認証局プロキシ 機能 サービスは自動的にアクティベートされません Cisco Unified Serviceability。

CAPF 機能を使用するには、最初のノードでこのサービスをアクティベートする必要があります。

Cisco CTL クライアントをインストールして設定する前にこのサービスをアクティベートしなかった場合は、CTL ファイルを更新する必要があります。

Cisco 認証局プロキシ機能 サービスを有効にすると、CAPF は CAPF に固有のキー ペアと証明書を自動的に生成します。 Cisco CTL クライアントがクラスタ内のスタンドアロンサーバまたはすべてのサーバにコピーする CAPF 証明書は、.0 拡張子を使用します。 CAPF 証明書は、CAPF 証明書が存在することの確認として、Cisco Unified Communications オペレーティングシステム GUI に表示されます。

アプリケーションユーザまたはエンドユーザの CAPF プロファイルのセットアップ

JTAPI/TAPI/CTI アプリケーション用のローカルで有効な証明書をインストール/アップグレード/トラブルシューティングする際の参照として、アプリケーションおよびエンドユーザ CAPF プロファイルの構成設定 を使用します。

ヒント エンド ユーザの CAPF プロファイルを設定する前に、アプリケーション ユーザの CAPF プロファイルを設定することをお勧めします。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから、次のいずれかのオプションを選択します:

a) **ユーザ管理 > ユーザ設定 > アプリケーション ユーザ CAPF プロファイル**
b) **[ユーザー管理（User Management）] > [ユーザー設定（User Settings）] > [エンドユーザー CAPF プロファイル（End User CAPF Profile）]**。

ステップ 2 次のいずれかの作業を実行します。

a) 既存のプロファイルを編集するには、 **検索** をクリックし、既存のプロファイルを選択します。
b) 新しいプロファイルを作成するには、[新規追加] をクリックします。
c) 既存のプロファイルの設定を新しいプロファイルにコピーするには、[**検索**] をクリックし、目的の設定を含む既存のプロファイルを選択します。 [**コピー**] をクリックして、これらの設定を含む新しいプロファイルの名前を付けます。 その後、必要に応じて新しいプロファイルを編集します。

ステップ 3 [アプリケーションユーザーおよびエンドユーザーの CAPF プロファイルの設定項目（Application and End User CAPF Profile Configuration Settings）] に記載されている適切な設定を入力します。

ステップ 4 **[保存]** をクリックします。

ステップ 5 追加の CAPF プロファイルを作成するには、この手順を繰り返します。 ユーザが必要な数のプロファイルを作成します。

[CCMQRTSecureSysUser]、**[IPMASecureSysUser]**、または **[WDSecureSysUser]** を **[アプリケーションユーザー CAPF プロファイル設定（Application User CAPF Profile Configuration）]** ウィンドウで設定している場合、**[サービスパラメータ（Service Parameters）]** を設定する必要があります。

CAPF の設定項目

次の表に、[アプリケーションユーザCAPFプロファイルの設定(Application User CAPF Profile Configuration)]ウィンドウと [エンドユーザCAPFプロファイルの設定(End User CAPF Profile Configuration)]ウィンドウでの CAPF 設定項目を示します。

表 *38 :* アプリケーション ユーザおよびエンドユーザの *CAPF* プロファイルの設定項目

設定	説明
[アプリケーションユーザ（Application User）]	ドロップダウンリストボックスから、**CAPF 操作用のアプリケーション ユーザ**を選択します。この設定には、設定されたアプリケーション ユーザが表示されます。 この設定は、**エンドユーザCAPFプロファイルの設定(End User CAPF Profile)** ウィンドウには表示されません。
[エンドユーザID(End User ID)]	ドロップダウンリストから、**CAPF 操作のエンド ユーザ**を選択します。 これによって、設定されたエンド ユーザが表示されます。 この設定は、**アプリケーションユーザCAPFプロファイルの設定(Application User CAPF Profile)** ウィンドウには表示されません。
インスタンス ID（Instance ID）	1 ～ 128 字の英数字（a ～z、A ～ Z、0 ～ 9）を入力します。 インスタンス ID は、認証操作のユーザーを指定します。 1 つのアプリケーションに対して複数の接続（インスタンス）を設定できます。アプリケーションと CTIManager との接続の安全を確保するには、アプリケーション PC（エンド ユーザの場合）またはサーバ（アプリケーション ユーザの場合）で実行されるインスタンスごとに一意の証明書があることを確認します。 このフィールドは、Web サービスおよびアプリケーションをサポートする CAPF Profile Instance ID for Secure Connection to CTIManager サービス パラメータに関連しています。

設定	説明
[証明書の操作(Certificate Operation)]	ドロップダウン リストから、次のオプションのいずれかを選択します。 • **[保留中の操作なし(No Pending Operation)]**：証明書の操作が発生しないときに表示されます。 (デフォルト設定) • **インストール/アップグレード(Install/Upgrade)**：アプリケーションのローカルで有効な証明書を新しくインストールするか、あるいは既存の証明書をアップグレードします。
認証モード（Authentication Mode）	証明書のインストールまたはアップグレード操作の認証モードは [認証ストリング(By Authentication String)] です。これは、ユーザまたは管理者が **JTAPI/TSP の初期設定**ウィンドウで CAPF 認証文字列を入力したときにだけ、ローカルで有効な証明書がインストール、アップグレード、またはトラブルシューティングされることを意味します。
認証文字列（Authentication String）	一意の文字列を手動で入力するか、あるいは**文字列を生成(Generate String)** ボタンをクリックして文字列を生成します。 文字列が 4 ～ 10 桁であることを確認してください。 ローカルで有効な証明書のインストールまたはアップグレードを実行する場合、アプリケーション PC の **[JTAPI/TSP 設定（JTAPI/TSP preferences）]**GUI に管理者が認証文字列を入力することが必要です。この文字列は、1 回だけ使用できます。あるインスタンスに文字列を使用した場合、その文字列をもう一度使用することはできません。
[文字列を生成(Generate String)]	CAPF が自動的に認証文字列を生成するよう設定するには、**文字列の生成**ボタンをクリックします。 4 ～ 10 桁の認証文字列が**認証文字列(Authentication String)** フィールドに表示されます。
キー順序（Key Order）	このフィールドは、CAPF のキーの並び方を指定します。 ドロップダウン リストから、次のいずれかの値を選択します： • **RSA のみ** • **EC のみ** • **EC 優先、RSA バックアップ** （注） **[キーオーダー（Key Order）]**、**[RSA キー サイズ（RSA Key Size）]**、および **[EC キー サイズ（EC Key Size）]** フィールドの値に基づいて電話を追加すると、デバイス セキュリティ プロファイルがその電話に関連付けられます。 256 ビットの **[EC キー サイズ（EC Key Size）]** 値で **[ECのみ（EC Only）]** 値を選択した場合は、デバイス セキュリティ プロファイルに **EC-256** 値が追加されます。

設定	説明
RSA キー サイズ（ビット）（RSA Key Size (Bits)）	ドロップダウンリストから、**512**、**1024**、**2048**、**3072**、または**4096**のいずれかの値を選択します。
EC キーサイズ（ビット）	ドロップダウンリストから、**256**、**384**、または**521**のいずれかの値を選択します。
[操作の完了期限(Operation Completes By)]	このフィールドは、すべての証明書操作をサポートし、操作を完了する必要がある期限の日付と時刻を指定します。 表示される値は、最初のノードに適用されます。 この設定は、証明書の操作を完了する必要がある期間のデフォルトの日数を指定する **[CAPF 操作有効期間（日数）（CAPF Operation Expires in (days)）]** エンタープライズパラメータと併用します。 このパラメータはいつでも更新できます。
[証明書の操作ステータス(Certificate Operation Status)]	このフィールドは、pending、failed、successful など、証明書操作の進行状況を表示します。 このフィールドに表示される情報は変更できません。

CAPF サービス パラメータの更新

サービスパラメータ ウィンドウには、Cisco 認証局プロキシ 機能 のオプション設定が含まれています。 CAPF 証明書の発行者、オンライン CA 接続設定、証明書の有効期間、キー サイズなどの設定を構成できます。

CAPF サービスパラメータが Cisco Unified Communications Manager Administration でアクティブと表示されるようにするには、 で 認証局プロキシ 機能 Cisco Unified Serviceability サービスを有効にします。

ヒント 電話で CAPF を使用したときに CAPF サービス パラメータを更新した場合は、サービス パラメータを再度更新する必要はありません。

CAPF サービスパラメータを更新するには、以下の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから、 **システム** > **サービスパラメータ** を選択します。

ステップ 2 [サーバ（Server）]ドロップダウン リストからサーバを選択します。

ヒント
クラスター内のパブリッシャノードを選択する必要があります。

ステップ 3 [サービス（Service）]ドロップダウン リストから、[Cisco 認証局プロキシ機能（アクティブ）（Cisco 認証局プロキシ 機能 (Active)）]を選択します。 サービス名の横に「「アクティブ」」と表示されていることを確認します。

ステップ 4 オンラインヘルプの説明に従って、 **CAPF（認証局プロキシ 機能）サービスパラメータ** を更新する。 **CAPF（認証局プロキシ機能）サービスパラメータ**のヘルプを表示するには、疑問符またはパラメータ名のリンクをクリックしてください。

ステップ 5 **Cisco 認証局プロキシ 機能** の Cisco Unified Serviceabilityサービスを再起動して変更を有効にしてください。

（注）
Certificate Authority Proxy 機能の設定方法の詳細は、 **Certificate Authority Proxy 機能** の章を参照してください。

アプリケーション ユーザ CAPF またはエンド ユーザ CAPF プロファイルの削除

Cisco Unified Communications Manager Administrationからアプリケーションユーザ CAPF プロファイルまたはエンドユーザ CAPF プロファイルを削除する前に、別のプロファイルをデバイスに適用するか、またはそのプロファイルを使用するすべてのデバイスを削除する必要があります。 このプロファイルを使用するデバイスを確認するには、**[セキュリティ プロファイルの設定（Security Profile Configuration）]** ウィンドウで **[関連リンク（Related Links）]** ドロップダウンメニューから **[依存関係レコード（Dependency Records）]** を選択し、**[実行（Go）]** をクリックします。

システムで依存関係レコード機能が有効になっていない場合、依存関係レコードの概要ウィンドウに、依存関係レコードを有効にするためのアクションを示すメッセージが表示されます。メッセージには、依存関係レコード機能に関連する高い CPU 消費に関する情報も表示されます。 依存関係レコードの詳細は、 Cisco Unified Communications Manager システム設定ガイドを参照してください。

このセクションでは、アプリケーションユーザ CAPF プロファイルまたはエンドユーザ CAPF プロファイルを Unified Communications Manager データベースから削除する方法について説明します。

手順

ステップ 1 [アプリケーション ユーザ CAPF プロファイル] または [エンド ユーザ CAPF プロファイル] を見つけます。

ステップ 2 次のいずれかの作業を実行します。

a) 複数のプロファイルを削除するには、[**検索と一覧表示**] ウィンドウ内で該当するチェックボックスの隣にあるチェックボックスを選択します。それから**選択項目を削除**をクリックします。 **[すべて選択(Select All)]** をクリックして **[選択項目の削除(Delete Selected)]** をクリックすると、この選択対象として設定可能なすべてのレコードを削除できます。
b) 単一のプロファイルを削除するには、**[検索と一覧（Find and List）]** ウィンドウで該当するプロファイルの隣にあるチェックボックスを選択し、次に**[選択項目を削除（Delete Selected）]** をクリックします。

ステップ 3 削除の確認が求められたら、[**OK**] をクリックして削除するか、または [**キャンセル**] をクリックして削除操作をキャンセルします。

CTI、JTAPI、および TAPI の保護

次の手順では、CTI/JTAPI/TAPI アプリケーションを保護するために実行するタスクを説明します。

手順

ステップ 1 CTI アプリケーションおよび JTAPI/TSP プラグインがインストールされ、実行中であることを確認します。

ヒント
アプリケーションユーザを [標準 CTI 有効] グループに割り当てます。

詳細については、次のドキュメントを参照してください。

- *Cisco JTAPI* インストールガイド用 *Unified Communications Manager*
- *Cisco TAPI* インストールガイド *Unified Communications Manager*

ステップ 2 次の Unified Communications Manager セキュリティ機能がインストールされていることを確認してください (インストールされていない場合は、これらの機能をインストールして設定します):

- CTL クライアントがインストールされているかどうかを確認し、CTL ファイルを実行します。
- CTL プロバイダー サービスがインストールされ、サービスがアクティベートされていることを確認します。
- CAPF サービスがインストールされ、有効になっていることを確認します。 必要に応じて、CAPF サービス パラメータを更新します。

ヒント

CAPF サービスは、CAPF 証明書を CTL ファイルに含めるために、 Cisco CTL Client が実行される必要があります。 電話の CAPF を使用したときにこれらのパラメータを更新した場合は、再度パラメータを更新する必要はありません。

- クラスターセキュリティ モードが混合モードに設定されていることを確認します。(クラスターセキュリティモードは、スタンドアロンサーバまたはクラスターのセキュリティ機能を構成します。)

  ヒント
  クラスタセキュリティモードが混合モードでない場合、CTI/JTAPI/TAPI アプリケーションは CTL ファイルにアクセスできません。

ステップ 3 エンドユーザとアプリケーションユーザを、必要な権限を含むアクセスコントロールグループに割り当てます。 ユーザを次のすべてのグループに割り当てることで、ユーザが CTI 接続で **TLS** および **SRTP** を使用できるようになります:

- [標準CTIを有効にする（Standard CTI Enabled）]
- 標準 CTI セキュア接続
- 標準 CTI SRTP 重要素材の受信許可

ヒント
CTI アプリケーションは、アプリケーションユーザーたはエンドユーザーのいずれか一方にのみ割り当てることができます。

ユーザは、 **標準 CTI 対応および標準 CTI セキュアコネクション** ユーザグループにすでに存在している必要があります。 アプリケーションまたはエンドユーザは、これら3つのグループの一部でない場合、SRTPセッションキーを受け取ることはできません。 詳細については、ユーザ アクセス コントロール グループ設定に関連するトピックを参照してください。

（注）
Cisco Unified Communications Manager Assistant、Cisco QRT、および Cisco Web Dialer は暗号化をサポートしていません。 CTIManager サービスに接続する CTI クライアントは、クライアントが音声パケットを送信する場合、暗号化をサポートしている可能性があります。

ステップ 4 エンドユーザおよびアプリケーションユーザの CAPF プロファイルを設定します。 詳細は **認証局プロキシ 機能** の章を参照してください。

ステップ 5 CTI/JTAPI/TAPI アプリケーションの対応するセキュリティ関連パラメータを有効にします。

アプリケーションユーザとエンドユーザをセキュリティ関連のアクセス コントロール グループに追加する

[標準 CTI セキュア接続] ユーザグループおよび [標準 CTI SRTP キーマテリアルの受信を許可する] ユーザグループは、デフォルトで Unified Communications Manager に表示されます。 これらのグループを削除することはできません。

ユーザの CTIManager への接続をセキュアにするには、アプリケーションユーザまたはエンドユーザを標準 CTI セキュア接続ユーザグループに追加する必要があります。 CTI アプリケーションは、アプリケーションユーザーたはエンドユーザーのいずれか一方にのみ割り当てることができます。

アプリケーションと CTIManager にメディアストリームをセキュアにさせたい場合、アプリケーションユーザまたはエンドユーザを、標準 CTI SRTP キーマテリアルの受信を許可ユーザグループに追加する必要があります。

アプリケーションとエンドユーザが SRTP を使用する前に、ユーザは TLS のベースライン構成として機能する、標準 CTI 対応および標準 CTI セキュア接続のユーザグループに属している必要があります。 SRTP 接続には TLS が必要です。 ユーザーがこれらのグループに属するようになったら、ユーザーを [標準 CTI SRTP 重要素材の受信許可（Standard CTI Allow Reception of SRTP Key Material）] ユーザーグループに追加できます。 アプリケーションが SRTP セッションキーを受信するには、アプリケーションまたはエンドユーザーが、**[標準CTIを有効にする（Standard CTI Enabled）]**、**[標準 CTI セキュア接続（Standard CTI Secure Connection）]**、および **[標準 CTI SRTP 重要素材の受信許可（Standard CTI Allow Reception of SRTP Key Material）]** の 3 つのグループに属している必要があります。

アプリケーションユーザである CCMQRTSecureSysUser、IPMASecureSysUser、および WDSecureSysUser を [標準 CTI SRTP キーマテリアルの受信を許可] ユーザグループに追加する必要はありません。 Cisco Unified Communications Manager Assistant、CiscoQRT、および Cisco Web Dialer は暗号化をサポートしていないためです。

ヒント ユーザグループからのアプリケーションまたはエンドユーザの削除については、 Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。 **[役割の設定（Role Configuration）]** ウィンドウのセキュリティ関連の設定については、『Cisco Unified Communications Manager アドミニストレーション ガイド』を参照してください。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから **ユーザ管理** > **ユーザグループ**を選択します。

ステップ 2 すべての **ユーザグループ**を表示するには、 **検索**をクリックします。

ステップ 3 目的に応じて、以下のいずれかのタスクを実行します。

a) アプリケーションまたはエンドユーザが [標準 CTI 有効] グループに存在していることを確認します。

b) アプリケーションユーザーを**[標準 CTI セキュア接続（Standard CTI Secure Connection）]** ユーザーグループに追加するには、**[標準 CTI セキュア接続（Standard CTI Secure Connection）]** リンクをクリックします。

c) アプリケーションユーザーを **[標標準 CTI SRTP 重要素材の受信許可（Standard CTI Allow Reception of SRTP Key Material）]** ユーザーグループに追加するには、**[標準 CTI SRTP 重要素材の受信許可（Standard CTI Allow Reception of SRTP Key Material）]** リンクをクリックします。

ステップ 4 グループにアプリケーションユーザーを追加するには、ステップ 5 から 7 を実行します。

ステップ 5 [**アプリケーションユーザをグループに追加]** をクリックします。

ステップ 6 アプリケーションユーザーを検索するには、検索基準を指定し、**[検索（Find）]** をクリックします。

検索条件を指定せずに [検索] をクリックすると、利用可能なすべてのオプションが表示されます。

ステップ 7 グループに追加するアプリケーションユーザーのチェックボックスを選択し、**[選択項目の追加（Add Selected）]** をクリックします。

ユーザは **ユーザグループ** ウィンドウに表示されます。

ステップ 8 エンドユーザーをグループに追加するには、ステップ 9 から 11 を実行します。

ステップ 9 **[ユーザをグループに追加] をクリックします**。

ステップ 10 エンドユーザーを検索するには、検索基準を指定し、**[検索（Find）]** をクリックします。

検索条件を指定せずに [検索] をクリックすると、利用可能なすべてのオプションが表示されます。

ステップ 11 グループに追加するエンドユーザーのチェックボックスを選択し、**[選択項目の追加（Add Selected）]** をクリックします。

ユーザは **ユーザグループ** ウィンドウに表示されます。

JTAPI/TAPI セキュリティ関連のサービスパラメータのセットアップ

Application User CAPF プロファイルまたは End User CAPF プロファイルを設定したら、 **Cisco IP Manager Assistant** サービスの以下のサービスパラメータを設定する必要があります:

- CTIManager Connection Security Flag
- CTIManager への安全な接続のための CAPF プロファイル インスタンス ID

サービスパラメータにアクセスするには、以下の手順を実行します。

手順

ステップ 1 Cisco Unified Communications Manager Administrationから **システム** > **サービスパラメータ** を選択します。

ステップ 2 **[サーバー（Server）]** ドロップダウンメニューから、**[Cisco IP Manager Assistant]** サービスがアクティブになっているサーバーを選択します。

ステップ 3 [サービス（Service）]ドロップダウン リストから、[Cisco IP Manager Assistant]サービスを選択します。

ステップ 4 パラメータが表示されたら、**[CTIManager Connection Security Flag]** と **[CTIManager へのセキュアな接続の CAPF プロファイルインスタンス ID（CAPF Profile Instance ID for Secure Connection to CTIManager）]** パラメータを見つけます。

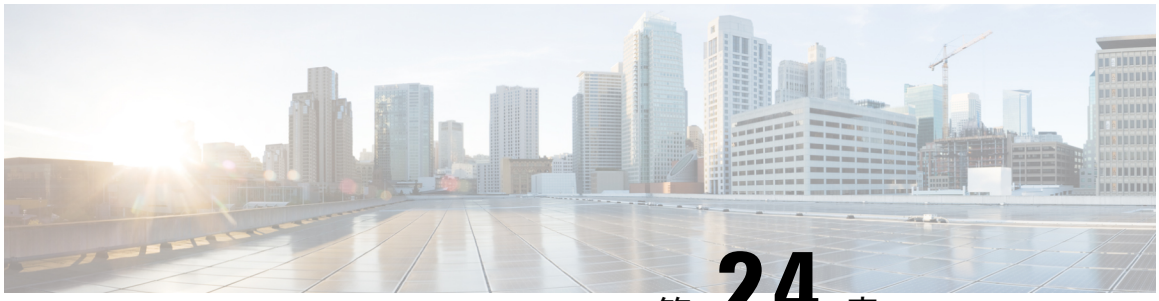
ステップ 5 パラメータを更新します。クエスチョンマークまたはパラメータ名のリンクをクリックすると表示されるヘルプを参照してください。

ステップ 6 **[保存（Save）]** をクリックします。

ステップ 7 サービスが有効になっている各サーバでこの手順を繰り返します。

アプリケーションまたはエンドユーザの証明書操作状況を表示する

証明書の処理状況は、特定の **[アプリケーションユーザー（Application User）]** または **[エンドユーザーの CAPF プロファイル設定（End User CAPF Profile configuration）]** ウィンドウ（**[検索/一覧表示（Find/List）]** ウィンドウではない）、または **[JTAPI/TSP の設定（JTAPI/TSP Preferences）]** GUI ウィンドウで確認できます。



第 24 章

安全な録画とモニタリング

- セキュアな通話のモニタリングと録音のセットアップについて （317 ページ）
- セキュア通話の監視と録音の設定 （318 ページ）

セキュアな通話のモニタリングと録音のセットアップについて

このセクションで説明されているように、安全な通話は監視および録音することができます。

- スーパーバイザは、セキュアな通話またはセキュアでない通話に対して、セキュアなモニタリング セッションを確立できます。
- 元の通話の通話セキュリティは、通話監視リクエストの結果として影響を受けたり、ダウングレードされたりすることはありません。
- モニタリング コールは、エージェントのデバイスの能力と同じセキュリティ レベルで確立および維持できる場合にのみ、処理を進めることができます。
- エージェントと顧客の間の元の通話は、モニタリング コールとは異なる暗号キーを持つ必要があります。モニタリングセッションでは、システムはスーパーバイザーに送信する前に、エージェントと顧客の混合音声を新しいキーで最初に暗号化します。

（注） Unified Communications Manager は、セキュアではないレコーダーの使用時の認証済み通話の通話録音をサポートしています。 セキュアなコール レコーダーを使用した通話の場合、レコーダーへのメディア ストリームが RTP にフォールバックできるように、レコーダーが SRTP フォールバックをサポートしている場合にのみ、録音が許可されます。

認証済み電話を使用する通話を録音するには:

- Cisco CallManager サービスパラメータの **認証済み電話録音**を **録音を許可**に設定します。この場合、通話は認証されますが、記録サーバへの接続は認証されず、暗号化されません。
- SIP OAuth 対応電話でセキュアな録音を行うには、Unified Communications Manager を常に混合モード クラスタ セキュリティで構成する必要があります。

セキュア通話の監視と録音の設定

この手順を使用して、安全な通話の監視と録音を設定します。

手順

ステップ 1 エージェントとスーパーバイザーの電話にセキュアな機能を設定します。

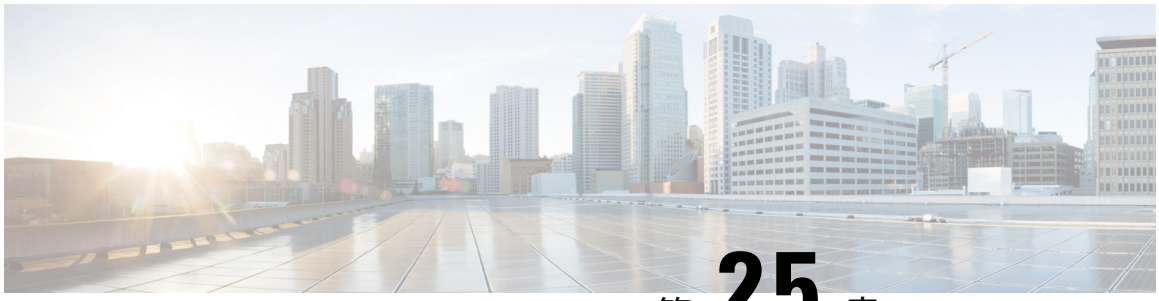
ステップ 2 次の設定でセキュアな SIP トランクを作成します。

- **端末のセキュリティモード** を暗号化に設定します。
- **セキュリティ状況を送信する** チェックボックスを選択します。
- [**SRTP 許可**] チェックボックスを選択します。
- レコーダーへの **TLS SIP トランク** を設定します。

ステップ 3 非セキュアな監視と録画の場合と同じように、監視と録画を構成します。

a) エージェントの電話にビルトイン ブリッジを設定します。
b) エージェントの電話で、[**ディレクトリ番号**] ページで、録音オプション (**自動通話録音有効 および アプリケーションによる通話録音有効**) を設定します。
c) レコーダーの **ルートパターン** を作成します。
d) **通話記録のプロファイル** をディレクトリ番号に追加します。
e) 必要に応じてモニタリング トーンと録音トーンをプロビジョニングします。

詳細な手順については、 「監視と録音」 の章を Cisco Unified Communications Manager 機能設定ガイドで参照してください。



第 25 章

VPN クライアント

- VPN クライアントの概要 （319 ページ）
- VPN クライアント設定のタスク フロー （319 ページ）

VPN クライアントの概要

Cisco Unified IP 電話 向け Cisco VPN Client により、在宅勤務の従業員のためのセキュアな VPN 接続が実現します。 Cisco VPN Client の設定はすべて Cisco Unified Communications Manager Administration で設定します。 社内で電話を設定したら、ユーザはその電話をブロードバンド ルータにつなぐだけで瞬時に組織のネットワークに接続できます。

（注） VPN メニューとそのオプションは、米国無制限輸出対象バージョンの Unified Communications Manager では利用できません。

VPN クライアント設定のタスク フロー

電話を事前にプロビジョニングし、社内ネットワーク内で初期接続を確立し、電話の設定を取得します。 設定はすでに電話に取り込まれているため、これ以降は VPN を使用して接続を確立できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco IOS の前提条件の完了 （321 ページ）	Cisco IOS の前提条件を満たします。 Cisco IOS VPN を設定するには、このアクションを実行します。
ステップ 2	IP Phone をサポートするための Cisco IOS SSL VPN の設定 （321 ページ）	IP Phone で VPN クライアントの Cisco IOS を設定します。 Cisco IOS VPN を

	コマンドまたはアクション	目的
		設定するには、このアクションを実行します。
ステップ 3	AnyConnect 用の ASA 前提条件への対応 （323 ページ）	AnyConnect 用の ASA 前提条件を満たします。 ASA VPN を設定するには、このアクションを実行します。
ステップ 4	IP Phone での VPN クライアント用の ASA の設定 （324 ページ）	IP Phone で VPN クライアントの ASA を設定します。 ASA VPN を設定するには、このアクションを実行します。
ステップ 5	VPN ゲートウェイごとに VPN コンセントレータを設定します。	ユーザがリモート電話のファームウェアや設定情報をアップグレードするときに遅延が長くなるのを回避するため、VPN コンセントレータはネットワーク内の TFTP サーバまたは Unified Communications Manager サーバの近くにセットアップします。 これがネットワーク内で不可能な場合、代替 TFTP サーバまたはロード サーバを VPN コンセントレータの横にセットアップすることもできます。
ステップ 6	VPN コンセントレータの証明書のアップロード （326 ページ）	VPN コンセントレータの証明書をアップロードします。
ステップ 7	VPN ゲートウェイの設定 （327 ページ）	VPN ゲートウェイを設定します。
ステップ 8	VPN グループの設定 （328 ページ）	VPN グループを作成した後、設定した VPN ゲートウェイのいずれかをそのグループに追加できます。
ステップ 9	次のいずれかを実行します。 • VPN プロファイルの設定 （329 ページ） • VPN 機能のパラメータの設定 （331 ページ）	VPN プロファイルを設定する必要があるのは、複数の VPN グループを使用している場合だけです。 [VPN Profle] フィールドは、[VPN Feature Configuration] フィールドよりも優先されます。
ステップ 10	共通の電話プロファイルへの VPN の詳細の追加 （333 ページ）	共通の電話プロファイルに VPN グループおよび VPN プロファイルを追加します。
ステップ 11	Cisco Unified IP 電話 のファームウェアを、VPN をサポートしているバージョンにアップグレードします。	To run the Cisco VPN client, a supported Cisco Unified IP 電話 must be running firmware release 9.0（2） or higher. ファームウェアのアップグレードの詳

	コマンドまたはアクション	目的
		細については、ご使用の Cisco Unified IP 電話 モデルの Unified Communications Manager に関する『*Cisco Unified IP Phone Administration Guide*』を参照してください。
ステップ 12	サポートされている Cisco Unified IP 電話 を使用して、VPN 接続を確立します。	Cisco Unified IP 電話 を VPN に接続します。

Cisco IOS の前提条件の完了

次の手順を使用して、Cisco IOS の前提条件を完了します。

手順

ステップ 1 Cisco IOS ソフトウェアバージョン 15.1(2)T 以降をインストールします。

機能セット/ライセンス：Universal（Data & Security & UC）for IOS ISR-G2 および ISR-G3

機能セット/ライセンス：Advanced Security for IOS ISR

ステップ 2 SSL VPN ライセンスをアクティベートします。

IP Phone をサポートするための Cisco IOS SSL VPN の設定

IP 電話をサポートするための Cisco IOS SSL VPN を実行するには、次の手順を使用します。

手順

ステップ 1 Cisco IOS をローカルで設定します。

a) ネットワーク インターフェイスを設定します。

例：

```
router(config)# interface GigabitEthernet0/0
router(config-if)# description "outside interface"
router(config-if)# ip address 10.1.1.1 255.255.255.0
router(config-if)# duplex auto
router(config-if)# speed auto
router(config-if)# no shutdown
router#show ip interface brief (shows interfaces summary)
```

b) 次のコマンドを使用してスタティック ルートとデフォルト ルートを設定します。

router(config)# **ip route** <*dest_ip*> < *mask*> < *gateway_ip*>

例：

```
router(config)# ip route 10.10.10.0 255.255.255.0 192.168.1.1
```

ステップ 2 CAPF 証明書を生成および登録して LSC の入った IP Phone を認証します。

ステップ 3 Unified Communications Manager から CAPF 証明書をインポートします。

a) [Cisco Unified OS Administration] から、**[セキュリティ（Security）] > [証明書の管理（Certificate Management）]** を選択します。

（注）
この場所は Unified Communications Manager のバージョンに基づきます。

b) Cisco_Manufacturing_CA および CAPF 証明書を見つけます。 .pem ファイルをダウンロードし、.txt ファイルとして保存します。

c) Cisco IOS ソフトウェアでトラストポイントを作成します。

```
hostname(config)# crypto pki trustpoint trustpoint_name
hostname(config-ca-trustpoint)# enrollment terminal
hostname(config)# crypto pki authenticate trustpoint
```

Base 64 で暗号化された CA 証明書を求められた場合は、ダウンロードした .pem ファイルのテキストを BEGIN 行および END 行とともにコピーし、貼り付けます。 この手順を他の証明書にも繰り返します。

d) 次の Cisco IOS 自己署名証明書を生成して Unified Communications Manager に登録するか、または CA からインポートした証明書で置き換えます。

- 自己署名証明書を生成します。

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# rsakeypair <name> 2048 2048
Router(ca-trustpoint)#authorization username subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- Unified Communications Manager の VPN プロファイルでホスト ID チェックを有効にして、自己署名証明書を生成します。

例：

```
Router> enable
Router# configure terminal
Router(config)# crypto key generate rsa general-keys label <name>
<exportable -optional>Router(config)# crypto pki trustpoint <name>
Router(ca-trustpoint)# enrollment selfsigned
Router(config-ca-trustpoint)# fqdn <full domain
name>Router(config-ca-trustpoint)# subject-name CN=<full domain
name>, CN=<IP>Router(ca-trustpoint)#authorization username
subjectname commonname
Router(ca-trustpoint)# crypto pki enroll <name>
Router(ca-trustpoint)# end
```

- 生成された証明書を Unified Communications Manager に登録します。

  例：

  ```
  Router(config)# crypto pki export <name> pem terminal
  ```

  端末からテキストをコピーして、.pem ファイルとして保存し、これを Cisco Unified OS の管理を使用して、Unified Communications Manager にアップロードします。

ステップ 4 AnyConnect を Cisco IOS にインストールします。

AnyConnect パッケージを cisco.com からダウンロードし、フラッシュにインストールします。

例：

```
router(config)#webvpn install svc
flash:/webvpn/anyconnect-win-2.3.2016-k9.pkg
```

ステップ 5 VPN 機能を設定します。

（注）
電話で証明書とパスワード認証の両方を使用する場合は、電話の MAC アドレスを使用してユーザを作成します。 ユーザ名の照合では、大文字と小文字が区別されます。 次に例を示します。

```
username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
```

AnyConnect 用の ASA 前提条件への対応

AnyConnect の前提条件を完了するには、次の手順を使用します。

手順

ステップ 1 ASA ソフトウェア（バージョン 8.0.4 以降）および互換性のある ASDM をインストールします。

ステップ 2 互換性のある AnyConnect パッケージをインストールします。

ステップ 3 ライセンスをアクティベートします。

a) 次のコマンドを実行して、現在のライセンスの機能を確認してください。

show activation-key detail

b) 必要な場合は、追加の SSL VPN セッションで新しいライセンスを取得し、Linksys 電話を有効にします。

ステップ 4 デフォルト以外の URL を持つトンネル グループが設定されていることを確認します。

```
tunnel-group phonevpn type remote-access
tunnel-group phonevpn general-attribute
  address-pool vpnpool
```

```
tunnel-group phonevpn webvpn-attributes
  group-url https://172.18.254.172/phonevpn enable
```

デフォルト以外の URL を設定するときは、次のことを考慮してください。

- ASA の IP アドレスにパブリック DNS エントリが含まれている場合、これを完全修飾ドメイン名（FQDN）に置き換えることができます。
- Unified Communications Manager では、VPN ゲートウェイに対して単一 URL（FQDN または IP アドレス）のみを使用できます。
- 証明書 CN またはサブジェクト代行名が必要な場合は、グループ URL の FQDN または IP アドレスを一致させます。
- ASA 証明書の CN や SAN が FQDN や IP アドレスと一致しない場合は、Unified Communications Manager のホスト ID チェックボックスをオフにします。

IP Phone での VPN クライアント用の ASA の設定

VPN クライアント用の ASA を IP 電話で設定するには、次の手順を使用します。

（注） ASA 証明書を置き換えると、Unified Communications Manager は使用できなくなります。

手順

ステップ 1 ローカル設定

a) ネットワーク インターフェイスを設定します。

例：

```
ciscoasa(config)# interface Ethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.89.79.135 255.255.255.0
ciscoasa(config-if)# duplex auto
ciscoasa(config-if)# speed auto
ciscoasa(config-if)# no shutdown
ciscoasa#show interface ip brief (shows interfaces summary)
```

b) スタティック ルートとデフォルト ルートを設定します。

ciscoasa(config)# **ルート** <interface_name> <ip_address> <netmask> <gateway_ip>

例：

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.89.79.129
```

c) DNS を設定します。

例：

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
```

ステップ 2 Unified Communications Manager と ASA に必要な証明書を生成して登録します。

Unified Communications Manager から次の証明書をインポートします。

- CallManager：TLS ハンドシェイク時の Cisco UCM の認証（混合モードのクラスタでのみ必要）。
- Cisco_Manufacturing_CA：製造元でインストールされる証明書（MIC）を使用した IP Phone の認証。
- CAPF：LSC を使用した IP Phone の認証。

これら Unified Communications Manager 証明書をインストールするには、次の手順を実行します。

a) [Cisco Unified OS Administration] から、**[セキュリティ（Security）]** > **[証明書の管理（Certificate Management）]** を選択します。

b) 証明書 Cisco_Manufacturing_CA と CAPF を見つけます。 `.pem` ファイルをダウンロードし、`.txt` ファイルとして保存します。

c) ASA でトラストポイントを作成します。

例：

```
ciscoasa(config)# crypto ca trustpoint trustpoint_name
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(config)# crypto ca authenticate trustpoint_name
```

Base 64 でエンコードされた CA 証明書を求められた場合は、ダウンロードした `.pem` ファイル内のテキストを BEGIN 行および END 行とともにコピーして、貼り付けます。 この手順を他の証明書にも繰り返します。

d) 次の ASA 自己署名証明書を生成して Unified Communications Manager に登録するか、または CA からインポートした証明書で置き換えます。

- 自己署名証明書を生成します。

  例：

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# keypair <name>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- Unified Communications Manager の VPN プロファイルでホスト ID チェックを有効にして、自己署名証明書を生成します。

  例：

```
ciscoasa> enable
ciscoasa# configure terminal
ciscoasa(config)# crypto key generate rsa general-keys label <name>
ciscoasa(config)# crypto ca trustpoint <name>
ciscoasa(ca-trustpoint)# enrollment self
ciscoasa(ca-trustpoint)# fqdn <full domain name>
ciscoasa(config-ca-trustpoint)# subject-name CN=<full domain name>,CN=<IP>
ciscoasa(config)# crypto ca enroll <name>
ciscoasa(config)# end
```

- 生成された証明書を Unified Communications Manager に登録します。

  例：

  ```
  ciscoasa(config)# crypto ca export <name> identity-certificate
  ```

  端末からテキストをコピーして、.pem ファイルとして保存し、Unified Communications Manager にアップロードします。

ステップ 3 VPN 機能を設定します。 以下に示すサンプル ASA 設定の概要を、設定のガイドとして利用できます。

（注）
電話で証明書とパスワード認証の両方を使用する場合は、電話の MAC アドレスを使用してユーザを作成します。 ユーザ名の照合では、大文字と小文字が区別されます。 次に例を示します。

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLGQIoxyCO4ti9 encrypted
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB attributes
ciscoasa(config-username)# vpn-group-policy GroupPhoneWebvpn
ciscoasa(config-username)#service-type remote-access
```

ASA 証明書の設定

ASA 証明書の設定に関する詳細は、「ASA 上の証明書認証を使用した AnyConnect VPN 電話の設定」を参照してください。

VPN コンセントレータの証明書のアップロード

VPN 機能をサポートするようにセットアップする際に、ASA で証明書を生成します。 生成された証明書を PC またはワークステーションにダウンロードしてから、この項で説明されている手順に従って、Unified Communications Manager にアップロードします。Unified Communications Manager は証明書を Phone-VPN-trust リストに保存します。

ASA は SSL ハンドシェイク時にこの証明書を送信し、Cisco Unified IP 電話 は、この証明書を電話と VPN 間の信頼リストに格納されている値と比較します。

ローカルで重要な証明書 (LSC) が Cisco Unified IP 電話 にインストールされている場合、デフォルトではその LSC が送信されます。

デバイス レベルの証明書認証を使用するには、ASA にルート MIC または CAPF 証明書をインストールして、Cisco Unified IP 電話 が信頼されるようにします。

Unified Communications Manager に証明書をアップロードするには、Cisco Unified OS Administration を使用します。

手順

ステップ 1 [Cisco Unified OS 管理（Cisco Unified OS Administration）] から、以下を選択します。**[セキュリティ] > [証明書の管理]**

ステップ 2 [証明書のアップロード]をクリックします。

ステップ 3 [証明書の目的（Certificate Purpose）] ドロップダウンリストで、[Phone-VPN-trust] を選択します。

ステップ 4 [ブラウズ（Browse）] をクリックして、アップロードするファイルを選択します。

ステップ 5 [ファイルのアップロード（Upload File）]をクリックします。

ステップ 6 アップロードする別のファイルを選択するか、[閉じる（Close）] をクリックします。

詳細については、「証明書の管理」の 章を参照 してください。

VPN ゲートウェイの設定

VPN ゲートウェイごとに VPN コンセントレータが設定されていることを確認します。 VPN コンセントレータの設定後、VPN コンセントレータの証明書をアップロードします。 詳細については、VPN コンセントレータの証明書のアップロード（326 ページ） を参照してください。

VPN ゲートウェイを設定するには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、以下を選択します。**[拡張機能（Advanced Features）] > [VPN] > [VPN ゲートウェイ（VPN Gateway）]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。

b) コピーする VPN ゲートウェイの横にある **[コピー（Copy）]**をクリックします。

c) 適切な VPN ゲートウェイを見つけて、設定を変更し、既存のプロファイルを更新します。

ステップ 3 [VPN Gateway Configuration] ウィンドウでフィールドを設定します。 詳細については、VPN クライアントの VPN ゲートウェイ フィールド （328 ページ） を参照してください。

ステップ 4 **[保存（Save）]** をクリックします。

VPN クライアントの VPN ゲートウェイ フィールド

VPN クライアントの VPN ゲートウェイフィールドについての説明をします。

表 *39 : VPN* クライアントの *VPN* ゲートウェイ フィールド

フィールド	説明
[VPNゲートウェイ名(VPN Gateway Name)]	VPN ゲートウェイの名前を入力します。
[VPNゲートウェイの説明(VPN Gateway Description)]	VPN ゲートウェイの説明を入力します。
[VPNゲートウェイのURL(VPN Gateway URL)]	ゲートウェイ内の主要な VPN コンセントレータの URL を入力します。 （注） VPN コンセントレータに 1 つのグループ URL を設定し、この URL をゲートウェイ URL として使用する必要があります。 設定情報については、次のような VPN コンセントレータのマニュアルを参照してください。 • 『*SSL VPN Client (SVC) on ASA with ASDM Configuration Example*』
[この場所のVPN証明書(VPN Certificates in this Location)]	上矢印キーおよび下矢印キーを使用して、証明書をゲートウェイに割り当てます。 ゲートウェイに証明書を割り当てないと、VPN クライアントはこのコンセントレータへの接続に失敗します。 （注） 最大 10 の証明書を 1 つの VPN ゲートウェイに割り当てることができます。また、各ゲートウェイに少なくとも 1 つの証明書を割り当てる必要があります。 電話と VPN 間の信頼性権限に関係付けられた証明書だけが、使用可能な VPN 証明書のリストに表示されます。

VPN グループの設定

VPN グループを設定するには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、以下を選択します。**[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN グループ（VPN Group）]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。
b) 既存の VPN グループをコピーする VPN グループの横にある **[コピー（copy）]** をクリックします。
c) 適切な VPN ゲートウェイを見つけて、設定を変更し、既存のプロファイルを更新します。

ステップ 3 [VPN Group Configuration] ウィンドウ内の各フィールドを設定します。 詳細については、フィールド説明の詳細について、VPN クライアントの VPN ゲートウェイ フィールド （328 ページ）を参照してください。

ステップ 4 **[保存（Save）]** をクリックします。

VPN クライアントの VPN グループ フィールド

この表では、VPN クライアントの VPN グループフィールドについて説明しています。

表 *40 : VPN* クライアントの *VPN* グループ フィールド

フィールド	定義
[VPNグループ名(VPN Group Name)]	VPN グループの名前を入力します。
[VPNグループの説明(VPN Group Description)]	VPN グループの説明を入力します。
[使用可能なすべてのVPNゲートウェイ(All Available VPN Gateways)]	スクロールして、使用可能なすべての VPN ゲートウェイを表示します。
[このVPNグループ内で選択されたゲートウェイ(Selected VPN Gateways in this VPN Group)]	上矢印ボタンと下矢印ボタンを使用して、使用可能な VPN ゲートウェイをこの VPN グループに入れたりグループから外したりします。 VPN クライアントで重要なエラーが発生し、特定の VPN ゲートウェイに接続できない場合は、リストの次の VPN ゲートウェイへの移動を試みます。 （注） 1 つの VPN グループに最大 3 つの VPN ゲートウェイを追加できます。 また、VPN グループ内の証明書数は、合計で 10 までです。

VPN プロファイルの設定

VPN プロファイルを設定するには、この手順を使用します。

手順

ステップ 1 Cisco Unified CM Administration から、以下を選択します。**[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN プロファイル（VPN Profile）]** を選択します。

ステップ 2 次のいずれかの作業を実行します。

a) **[新規追加（Add New）]** をクリックして、新しいプロファイルを設定します。

b) 既存のプロファイルをコピーする VPN プロファイルの横にある **[コピー （copy ）]** をクリックします。

c) 既存のプロファイルを更新するには、該当するフィルタを [Find VPN Profile Where] で指定し、[検索（Find）] をクリックして設定を変更します。

ステップ 3 [VPN Profile Configuration] ウィンドウで各フィールドを設定します。 詳細については、フィールド説明の詳細について、VPN クライアントの VPN プロファイル フィールド （330 ページ）を参照してください。

ステップ 4 **[保存（Save）]** をクリックします。

VPN クライアントの VPN プロファイル フィールド

この表では、VPN プロファイルフィールドの詳細について説明します。

表 *41 : VPN* プロファイル フィールドの詳細

フィールド	定義
名前	VPN プロファイルの名前を入力します。
説明	VPN プロファイルの説明を入力します。
[自動ネットワーク検出を有効化(Enable Auto Network Detect)]	このチェックボックスをオンにすると、VPN クライアントは、社内ネットワーク外にあることが検出された場合に限り実行できます。 デフォルト：[無効(Disabled)]
MTU	最大伝送ユニット（MTU）のサイズをバイト数で入力します。 デフォルト：1290 バイト
[接続の失敗(Fail to Connect)]	VPN トンネルの作成中に、ログインまたは接続操作が完了するまで待機する時間を指定します。 デフォルト：30 秒

フィールド	定義
[ホストIDチェックを有効化(Enable Host ID Check)]	このチェックボックスがオンの場合、ゲートウェイ証明書の subjectAltName または CN が、VPN クライアントの接続先の URL と一致している必要があります。 デフォルト：[有効(Enabled)]
[クライアント認証方式(Client Authentication Method)]	ドロップダウン リストから、クライアント認証方式を選択します。 • [ユーザおよびパスワード(User and password)] • [パスワードのみ(Password only)] • [証明書(Certificate)]（LSC または MIC）
[永続的パスワードを有効化(Enable Password Persistence)]	このチェックボックスをオンにすると、ログインの失敗、ユーザーによる手動のパスワードのクリア、電話のリセット、または電源が切れるまで、ユーザーのパスワードは電話に保存されます。

VPN 機能のパラメータの設定

手順

ステップ 1 Cisco Unified CM Administration から、以下を選択します。**[拡張機能（Advanced Features）]** > **[VPN]** > **[VPN 機能設定（VPN Feature Configuration）]**。

ステップ 2 [VPN Feature Configuration] ウィンドウのフィールドを設定します。 詳細については、VPN 機能のパラメータ （331 ページ） を参照してください。

ステップ 3 **[保存]** をクリックします。

次の作業を行います。

- Cisco Unified IP Phone のファームウェアを、VPN をサポートしているバージョンにアップグレードします。 ファームウェアのアップグレード方法の詳細については、ご使用の Cisco Unified IP 電話 モデルの『*Cisco Unified IP Phone Administration Guide*』を参照してください。
- サポートされている Cisco Unified IP 電話 を使用して、VPN 接続を確立します。

VPN 機能のパラメータ

VPN 機能パラメータの説明を表に示します。

表 *42 : VPN* 機能のパラメータ

フィールド	デフォルト
[自動ネットワーク検出を有効化(Enable Auto Network Detect)]	[True] の場合、VPN クライアントは、社内ネットワーク外にあることが検出された場合に限り実行できます。 デフォルト：False
MTU	最大伝送単位を指定します。 デフォルト：1290 バイト 最小値：256 バイト 最大値：1406 バイト
[キープ アライブ（Keep Alive）]	キープ アライブ メッセージを送信する間隔を指定します。 （注） この値がゼロ以外であり、かつ Unified Communications Manager で指定された値よりも小さい場合、VPN コンセントレータのキープ アライブ設定によってこの設定が上書きされます。 デフォルト：60 秒 最小値：0 秒 最大値：120 秒
[接続の失敗(Fail to Connect)]	VPN トンネルの作成中に、ログインまたは接続操作が完了するまで待機する時間を指定します。 デフォルト：30 秒 最小値：0 秒 最大値：600 秒
[クライアント認証方式(Client Authentication Method)]	ドロップダウン リストから、クライアント認証方式を選択します。 • [ユーザおよびパスワード(User and password)] • [パスワードのみ(Password only)] • [証明書(Certificate)]（LSC または MIC） デフォルト：[ユーザおよびパスワード(User and password)]

フィールド	デフォルト
[永続的パスワードを有効化(Enable Password Persistence)]	Trueの場合、リセットにResetボタンまたは「**#**」が使用されていると、ユーザーのパスワードが電話機に保存されます。 電話機の電源が切れた場合、または工場出荷時の設定にリセットされた場合、パスワードは保存されず、電話機は認証情報の入力を求めるプロンプトを表示します。 デフォルト：False
[ホストIDチェックを有効化(Enable Host ID Check)]	[True] の場合、ゲートウェイ証明書の subjectAltName または CN が、VPN クライアントの接続先の URL と一致している必要があります。 デフォルト：[True]

共通の電話プロファイルへの VPN の詳細の追加

一般的な電話プロファイルに VPN の詳細を追加するには、次の手順を使用します。

手順

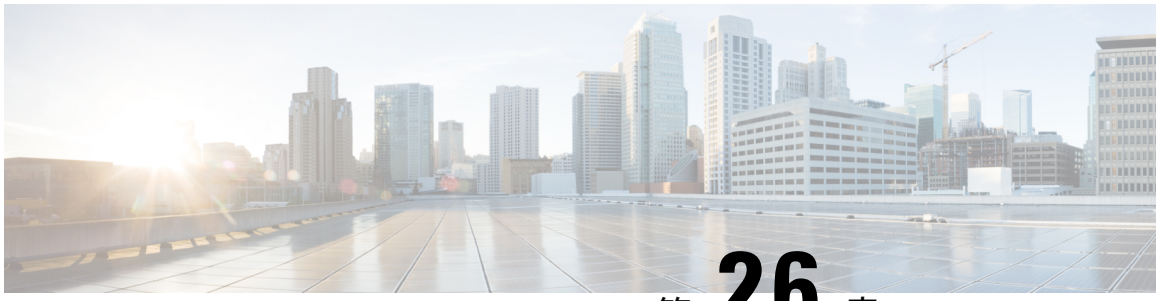
ステップ 1 Cisco Unified CM Administration から、以下を選択します。**[デバイス（Device）] > [デバイスの設定（Device Settings）] > [共通の電話プロファイル（Common Phone Profile）]**。

ステップ 2 [**検索（Find**）] をクリックして、VPNの詳細を追加する共通電話プロファイルを選択します。

ステップ 3 [VPN情報（VPN Information）] セクションで、適切な [VPNグループ（VPN Group）] および [VPNプロファイル（VPN Profile）] を選択します。

ステップ 4 [**保存（Save**）] と [**設定の適用（Apply Config**）] をクリックします。

ステップ 5 設定の適用ウィンドウで [**OK**] をクリックします。



第 26 章

オペレーティングシステムとセキュリティ強化

• セキュリティの強化 （335 ページ）

セキュリティの強化

Unified Communications Manager 12.5SU3 のセキュリティ機能の概要を以下に示します。 以下の一部の項目は、Cisco の標準製品マニュアルの更新が予定される前に提供されています。

Unified Communications Manager VMware vSphere ESXi に基づく仮想ハードウェア上で仮想マシンとして実行されます。 従来のサーバベースの製品とは異なり、Unified Communications Manager は、クローズドシステムの、即時使用可能な「アプライアンス」ワークロードとして配布されるソフトウェア製品であり、次の機能を備えています:

- 攻撃対象領域を減らす
- より安定した、より高性能な構成を提供
- 構成エラーによる脆弱性を回避
- 管理と修正メンテナンスを簡素化、OS / DB のスキル セットを必要とせずに

Unified Communications Manager ワークロードレイヤー強化のハイライトには以下のようなものがあります:

- Unified Communications Manager 汎用 / オープンシステムのワークロードではありません。
  - 汎用 OS ディストリビューションは使用しません。
    - 未使用のモジュールはイメージから除外され、未使用のサービスは無効化/削除されます。
    - 特定のモジュールに独自の強化変更を加えます (たとえば、OpenSSL は Cisco の Security and Trust Organization によって強化され、その結果として得られる CiscoSSL は製品に組み込まれています)。

- ゲスト OS、データベース、ランタイム、その他のワークロード ソフトウェア コンポーネントへのネイティブ インターフェイスは公開されません。
  - それらは削除されるか、非表示になってロックダウンされます。
  - アクセスは、Cisco が提供するブラウザベースの GUI、CLI、または API を通じてのみ行われます。これらのインターフェイスをセキュリティ保護するためのさまざまなメカニズムがあります (例: SSH 経由の CLI、またはセキュア FTP 経由のワークロードへのファイルの取り込み)。
- 製品は、アプリケーションの操作、保守、セキュリティ保護、管理に必要なすべてのソフトウェアを含む、慎重に制御されたスタックで構成されています。 Cisco が提供し、デジタル署名したイメージを使用して、このソフトウェアのすべてを指定、インストール、更新します。
- 上記のすべての情報は、Cisco セキュア製品ライフサイクル開発アプローチの開発およびテスト プロセスの対象となります。次を参照: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-secure-development-lifecycle.pdf

- Unified Communications Manager ワークロードレイヤーは、Cisco 以外のソフトウェアの挿入、および上記の管理対象Cisco が提供するインタフェース以外のソフトウェアの更新/変更をサポートしていません。
  - ワークロード内のすべてのソフトウェアはCisco により提供され、デジタル署名され、一枚岩のイメージ (.ISO ファイル) として配信されます。
  - ソフトウェアをインストール、アップグレード、および更新する唯一の方法は、Cisco が提供する .ISO または .COP ファイルを使用することです。
  - .ISO ファイルは、Cisco イメージ中のソフトウェア要素の 1 つ、一部、またはすべてをインストールまたは更新します。.COP ファイルは、単一の要素 (一般的にはユーザロケールと電話ファームウェアの更新) の更新に使用されます。
  - 以下は有効になっていない、または可能ではありません。
    - アンチウイルスクライアント、UPS エージェント、管理エージェントなどのオンボードエージェント。
    - 顧客がアップロード可能なソフトウェアまたは外部からアップロード可能なソフトウェア。
    - サードパーティのアプリケーション。

- ワークロード内のゲスト OS への「ルート アクセス」が有効になっていません。
  - 顧客は Cisco が提供する GUI、CLI、および/または API で認証を使用します。
  - ワークロードに公開されるすべてのインターフェイスはセキュリティ保護されています (例えば、パスワード複雑度ルールの強制、telnet の代わりの SSH、構成可能な最小バージョンの TLS 1.2 など)。

- フィールドでの通常のGUI/CLI/APIでは修正できない緊急事態の場合、顧客は一時的な「リモートアカウント」をセットアップして、Cisco Technical Assistance Center (TAC)エキスパートがルートアクセスを取得できるようにすることができます。顧客は制御を維持し、自動期限付きアカウントをオンまたはオフにすることができます。TACによって実行され、記録されるすべてのアクションを通じて、顧客はTAC担当者が何を行っているかを確認することができます。

- 組み込みの侵入防御機能:
  - SELinux 保護モード。ホストベースの侵入防御を提供します。
    - SELinux保護モードはデフォルトで有効になっています。このモードは、アプリケーション、デーモンなどをジョブ実行に必要な「最小限の権限」に制限する必須のアクセス制御を実施します。
  - IPtables ホストベースのファイアウォール:
    - IPtables はデフォルトで有効になっています。
    - ルールは Cisco Service Activation によって調整され、適切なポートを開くようにし、そのサーバで使用されているサービスの適切なレート制限が適用されます。
    - IPtable ルールは次のコマンドを使用して表示できます:
      - **utils ファイアウォール ipv4 リスト**
      - **utils ファイアウォール ipv6 リスト**

上記の強化機能に加えて、 Unified Communications Manager システムは OS、DB、アプリケーションソフトウェアのセキュリティ監査ログを行います。3つのセキュリティ監査ログが含まれます:

- Linux の監査ログ。
- Unified CM アプリケーション監査ログ。
- Informix データベース監査ログ。

組織の情報セキュリティ要件に準拠するようにシステムを構成することが可能な構成設定もあります。システム管理者による構成が可能なセキュリティ設定およびユーティリティには以下が含まれます:

- パスワードポリシーを定義する。 すべてのパスワードと PIN はハッシュ化または暗号化され、クリア テキストでは保存されません。
- アカウントのロックアウト設定と資格情報ポリシー。
- 警告バナーテキスト。
- シグナリングとメディアの TLS/SRTP を有効にします。

- 電話堅牢化の設定。
- TLS を使用しない接続を保護するための IPSec。
- 自己署名 PKI 証明書を CA 署名に変更する。
- FIPS モードまたは Common Criteria モードを有効にする。
- スマートカードまたは生体認証リーダーのサポートを含む SAML シングルサインオンを有効にする。
- すべてのネットワーク接続、プロセス、アクティブなパッケージを表示します。
  - 「show ネットワーク ステータス 詳細 nodns すべて」開いているポートの詳細を取得します。「netstat -an」Unix コマンドと同等です。
  - 「show process list detail」すべてのプロセスのリストと各プロセスに関する重要な情報を取得します。「ps -ef」Unix コマンドと同等です。
  - "show packages active" インストールされているアクティブなパッケージの名前とバージョンを表示します。

構成可能なセキュリティオプションの詳細については、『Cisco Unified Communications Manager セキュリティガイド』を参照してください。

Cisco の UC 製品は、定期的にテストおよび検証されており、以下を含むさまざまな政府認証に準拠しています。

- 米国国防総省情報ネットワーク承認製品リスト (DoDIN APL)
- FIPS 140-2 レベル 1
- FedRAMP
- コモン クライテリア
- 適用可能な米国国防総省セキュリティ技術導入ガイド (STIGs)

Cisco 政府認証の詳細については、次を参照してください。
https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications.html

セキュリティの脆弱性の警告と管理に関する全作業は、Cisco Product Security Incident Response Team (PSIRT) の管轄下にあります。 Unified Communications Manager Cisco PSIRT は、Cisco 製品に関連するセキュリティの脆弱性と問題に関する情報の受領、調査、公開レポートを管理する専任のグローバル チームです。 次のことを行ってください:

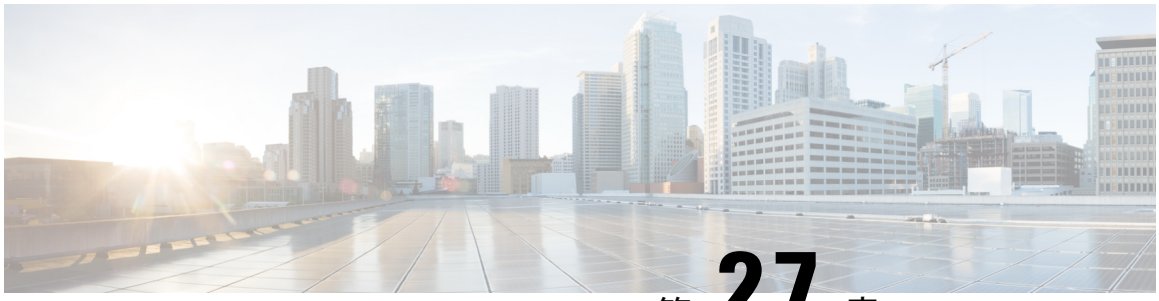
- Cisco セキュリティ勧告と警告ページ (https://tools.cisco.com/security/center/publicationListing.x) で、展開に影響する可能性があるセキュリティ問題に関する警告を監視してください。
- 特定の PSIRT の Cisco.com セキュリティ アドバイザリ ページを見て、影響を受ける製品、回避策、恒久的な修正を確認してください。

詳細については、次を参照してください。
https://tools.cisco.com/security/center/resources/security_vulnerability_policy.html

第 V 部

トラブルシューティング

- セキュリティのトラブルシューティングの概要 （341 ページ）



第 27 章

セキュリティのトラブルシューティングの概要

- Remote Access （341 ページ）
- Cisco Secure Telnet （342 ページ）
- リモート アカウントの設定 （343 ページ）

Remote Access

リモート アクセスを使用すると、必要なすべての装置に対して Terminal Services セッション（リモート ポート 3389）、HTTP セッション（リモート ポート 80）、および Telnet セッション（リモート ポート 23）を確立できます。

⚠

注意 ダイヤルインを設定する場合は、システムに対する脆弱性となるため、**login:cisco** または **password:cisco** は使用しないでください。

TAC エンジニアが次のいずれかの方法を使用してデバイスにリモート アクセスすることを許可すると、多くの問題を非常に迅速に解決できます。

- パブリック IP アドレスが設定された装置
- ダイヤルイン アクセス：（プリファレンスの高い順に）アナログ モデム、統合デジタル通信網（ISDN）モデム、バーチャル プライベート ネットワーク（VPN）
- ネットワーク アドレス変換（NAT）：プライベート IP アドレスが設定された装置へのアクセスを可能にする IOS およびプライベート インターネット エクスチェンジ（PIX）。

エンジニアの介入時にファイアウォールによって IOS トラフィックと PIX トラフィックが遮断されないこと、およびサーバ上で Terminal Services などの必要なすべてのサービスが開始されていることを確認してください。

（注） TACでは、すべてのアクセス情報は厳重に管理されます。また、お客様の同意なしにシステムを変更することはありません。

Cisco Secure Telnet

CIsco サービスエンジニア（CSE）は、Cisco Secure Telnet を使用して、サイト上の Unified Communications Manager サーバーに対して透過的にファイアウォールアクセスを実行できます。

Cisco Secure Telnet は、Cisco のファイアウォール内部で Telnet クライアントをイネーブル化することによって、ファイアウォールで稼働する Telnet デーモンに接続します。 このセキュアな接続により、ファイアウォールを変更せずに、Unified Communications Managerサーバの監視およびメンテナンスをリモートで行うことができます。

（注） Cisco は、許可があった場合にだけお客様のネットワークにアクセスします。 サイトに、このプロセスの開始を支援するネットワーク管理者を配置する必要があります。

ファイアウォールによる保護

ほとんどすべての内部ネットワークでは、外部から内部のホストシステムへのアクセスを制限するためにファイアウォールアプリケーションが使用されています。これらのアプリケーションでは、ネットワークとパブリックインターネットとの間のIP接続を制限することによって、ネットワークが保護されます。

ファイアウォールでは、許可するように明示的に再設定しないかぎり、外部から開始されるTCP/IP 接続が自動的にブロックされます。

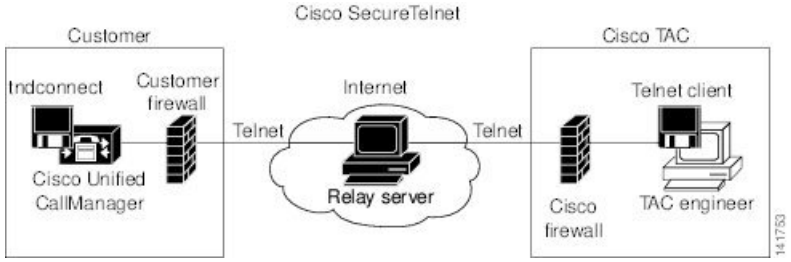
通常、企業ネットワークではパブリックインターネットとの通信が許可されますが、ファイアウォール内部から外部ホストに向けて開始される接続だけが許可されます。

Cisco Secure Telnet の設計

Cisco Secure Telnet では、ファイアウォールの内側から簡単に Telnet 接続を開始できるという技術を活用しています。 外部のプロキシ マシンを使用して、ファイアウォールの内側からのTCP/IP 通信が *Cisco Technical Assistance Center* (TAC) にある別のファイアウォールの内側のホストへとリレーされます。

このリレーサーバを使用することによって、両方のファイアウォールの完全性が維持され、また保護されたリモート システム間の安全な通信がサポートされます。

図 *1 : Cisco Secure Telnet* システム



Cisco Secure Telnet の構造

外部のリレーサーバーによって、お客様のネットワークと Cisco との間に Telnet トンネルが構築され、接続が確立されます。 これにより、Unified Communications Managerサーバの IP アドレスおよびパスワード識別子を CSE に送信できます。

（注） パスワードは、管理者と CSE が相互に同意した文字列です。

管理者は、Telnet トンネルを開始することによって、プロセスを開始します。これにより、ファイアウォールの内部からパブリック インターネット上のリレー サーバへの TCP 接続が確立されます。 次に、Telnet トンネルによって、ローカルの Telnet サーバへの別の接続が確立され、エンティティ間の双方向のリンクが作成されます。

（注） Cisco TAC の Telnet クライアントは、Windows NT および Windows 2000 上で動作するシステム、または UNIX オペレーティング システムに準拠して動作します。

ローカル サイトの Cisco Communications Manager がパスワードを受け入れると、Cisco TAC で実行されている Telnet クライアントは、ローカル ファイアウォールの内側で動作する Telnet デーモンに接続します。 この結果確立される透過的接続によって、マシンがローカルで使用されている場合と同様にアクセスできるようになります。

安定的な Telnet 接続が確立されると、CSE は、Unified Communications Managerサーバに対してメンテナンス タスク、診断タスク、およびトラブルシューティング タスクを実行するためのあらゆるリモート有用性機能を導入できます。

CSE が送信するコマンドおよびUnified Communications Managerサーバから発行される応答を確認することはできますが、コマンドや応答が常に完全な形式で表示されるとは限りません。

リモート アカウントの設定

Cisco サポートがトラブルシューティングのためにご使用のシステムに一時的にアクセスできるよう、Unified Communications Manager でリモートアカウントを設定します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）]で、**[サービス（Services）]** > **[リモート サポート（Remote Support）]** を選択します。

ステップ 2 [アカウント名（Account Name）]フィールドに、リモート アカウントの名前を入力します。

ステップ 3 [アカウントの有効期限（Account Duration）]フィールドに、アカウントの有効期限を日数で入力します。

ステップ 4 **[保存（Save）]** をクリックします。
システムは、暗号化パス フレーズを生成します。

ステップ 5 Cisco サポート担当者に連絡して、リモートサポートアカウント名とパスフレーズを提供します。

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。