



Cisco Unified Communications Manager リリース 15 セキュリティ ガイド

初版：2023 年 12 月 18 日

最終更新：2024 年 1 月 17 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 NON-INFRINGEMENT 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)

© 2023–2024 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 表記法 xx 法令順守 xxi |
| 第 1 章 | 新機能および変更された機能に関する情報 1 新機能および変更された機能に関する情報 1 |
| 第 1 部 : | Unified CM のセキュリティの概要 3 |
| 第 2 章 | 概要 5 システム要件 5 ベストプラクティス 5 デバイスのリセット、サーバとクラスタのリブート、およびサービスの再起動 6 デバイス、サーバ、クラスタ、およびサービスのリセット 7 割り込みセットアップによるメディア暗号化 8 一般的なアイコン 8 |
| 第 3 章 | コンフィギュレーション 11 セキュリティの設定 11 |
| 第 4 章 | デフォルトのセキュリティ 15 デフォルトのセキュリティの概要 15 |

| | |
|---|----|
| 初期信頼リスト | 15 |
| ITLRecovery 証明書の証明書管理の変更 | 17 |
| ITLRecovery 証明書 | 17 |
| 連携動作と制限事項 | 18 |
| 信頼検証サービス | 18 |
| 認証、整合性、および許可 | 19 |
| イメージ認証 | 19 |
| デバイス認証 | 20 |
| ファイル認証 | 20 |
| シグナリング認証 | 21 |
| ダイジェスト認証 | 21 |
| 認証 | 23 |
| NMAP スキャン操作 | 24 |
| 自動登録 | 25 |
| Cisco Unified Communications Manager と ITL ファイルを使用したクラスタ間での IP フォンの移行 | 25 |
| 暗号化 | 26 |
| セキュア エンド ユーザ ログイン クレデンシヤル | 26 |
| シグナリング暗号化 | 27 |
| メディア暗号化 | 28 |
| Secure Hash Algorithm (SHA-2) の SCCP ゲートウェイおよびハードウェア会議ブリッジ | 29 |
| TLS および SIP SRTP に対する AES 256 暗号化のサポート | 31 |
| TLS での AES 256 および SHA 2 のサポート | 32 |
| SRTP SIP コールシグナリングでの AES 256 のサポート | 33 |
| Cisco Unified Communications Manager の要件 | 34 |
| 連携動作と制限事項 | 34 |
| AES 80 ビット認証サポート | 34 |
| メディアストリーミングデバイスとの SRTP 暗号の不一致 | 35 |
| 自己暗号化ドライブ | 36 |
| 設定ファイルの暗号化 | 36 |
| デフォルトのセキュリティ管理タスク | 37 |

| | |
|--------------------------------|----|
| Cisco Unified IP 電話のITLファイルの更新 | 37 |
| ITLファイルステータスの取得 | 38 |
| Cisco Unified IP 電話サポートリストの取得 | 38 |
| 8.0より前のリリースへのクラスタのロールバック | 39 |
| 復帰後のリリース8.6以降へのスイッチバック | 40 |
| ITLファイルの一括リセットの実行 | 41 |
| CTL ローカルキーのリセット | 42 |
| ITLRecovery 証明書の有効期間の表示 | 42 |
| 認証と暗号化のセットアップ | 43 |

第 II 部 : **基本的なシステムセキュリティ** 45

第 5 章 **証明書** 47

| | |
|-------------------------------|----|
| 証明書の管理 | 47 |
| 証明書概要 | 47 |
| 証明書タイプ | 49 |
| 電話機の証明書タイプ | 49 |
| サーバ証明書のタイプ | 50 |
| サードパーティー CA 署名付き証明書 | 52 |
| 外部 CA からの証明書のサポート | 52 |
| 証明書署名要求のキー用途拡張 | 53 |
| 証明書タスク | 54 |
| 証明書の一括エクスポート | 55 |
| 証明書の表示 | 56 |
| 証明書のダウンロード | 56 |
| 中間証明書のインストール | 57 |
| 信頼証明書の削除 | 57 |
| 証明書署名要求の生成 | 58 |
| 自己署名証明書の生成 | 61 |
| 証明書の再作成 | 65 |
| 信頼ストアへの認証局署名済み CAPF ルート証明書の追加 | 73 |

| | |
|-------------------------------------|----|
| CTL ファイルの更新 | 74 |
| 連携動作と制限事項 | 74 |
| 証明書のモニタリングと失効タスクのフロー | 74 |
| 証明書モニタリングの概要 | 75 |
| 証明書モニタリングの設定 | 75 |
| 証明書失効の概要 | 75 |
| 証明書失効の設定 | 75 |
| 簡素化された証明書管理 | 78 |
| 簡略化された証明書管理の概要 | 78 |
| 簡素化された証明書管理ユーザインターフェイスの更新 | 79 |
| CallManager 用のマルチサーバ Tomcat 証明書の再利用 | 80 |

第 6 章

Certificate Authority Proxy Function 81

| | |
|---------------------------------|----|
| 認証局プロキシ機能の概要 | 81 |
| 認証局プロキシ機能の設定タスクフロー | 83 |
| 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 | 84 |
| 認証局 (CA) ルート証明書のアップロード | 85 |
| オンライン認証局の設定 | 86 |
| オフライン認証局の設定の設定 | 87 |
| CAPF サービスのアクティブ化または再起動 | 88 |
| ユニバーサル デバイス テンプレートでの CAPD 設定の構成 | 89 |
| 一括管理による CAPF 設定の更新 | 90 |
| 電話機の CAPF 設定の構成 | 91 |
| キープアライブ タイマーの設定 | 92 |
| 認証局プロキシ機能の管理タスクフロー | 92 |
| 古い LSC レポートの実行 | 93 |
| CAPF 経由の LSC 生成 | 93 |
| 保留中の CSR リストの表示 | 94 |
| 古い LSC 証明書の削除 | 94 |
| CAPF システムの連携動作 | 95 |
| 7942 および 7962 電話機での CAPF の例 | 96 |

IPv6 アドレッシングとの CAPF のインタラクション 97

第 7 章

セキュリティモード 101

- セキュリティモードの概要 101
- 非セキュアモード (デフォルトモード) 101
- セキュアモードの設定 101
 - 混合モード 102
 - セキュリティモードの確認 103
 - CTL ファイルの SAST 役割 104
 - SIP OAuth モード 104
 - CLI を使用した SIP OAuth 設定 105

第 8 章

SIP OAuth モード 107

- SIP OAuth モードの概要 107
- SIP OAuth モードの前提条件 108
- SIP OAuth モードの設定タスク フロー 109
 - Phone Edge TrustへのCA証明書のアップロード 110
 - デバイスの OAuth アクセストークンを有効にする 110
 - 更新ログインの設定 111
 - OAuth ポートの設定 111
 - OAuth Connection を Expressway-C に設定 112
 - SIP OAuth モードの有効化 113
 - Cisco CallManager サービスの再起動 113
 - 電話セキュリティプロファイルでデバイスセキュリティモードを設定する 113
 - SIPOAuth 登録済み電話を MRA モード用に構成する 114

第 9 章

TFTP 暗号化 117

- 暗号化された TFTP 設定ファイルの概要 117
 - 暗号化された TFTP 設定ファイルのヒント 118
- 電話機の設定ファイルの暗号化のタスクフロー 119
 - TFTP 暗号化の有効化 120

| | |
|---------------------------|-----|
| SHA-512 署名アルゴリズムの設定 | 120 |
| LSC または MIC 証明書のインストールの確認 | 121 |
| CTL ファイルの更新 | 122 |
| サービスの再起動 | 122 |
| 電話のリセット | 122 |
| 暗号化された TFTP 設定ファイルの無効化 | 123 |

第 10 章**暗号管理 125**

| | |
|------------|-----|
| 暗号管理 | 125 |
| 推奨される暗号 | 127 |
| 暗号ストリングの設定 | 128 |
| 暗号の制限 | 131 |
| 暗号の制限 | 144 |

第 11 章**電話機のセキュリティ 145**

| | |
|--|-----|
| 電話のセキュリティの概要 | 145 |
| 電話機のセキュリティ強化の概要 | 146 |
| 電話のセキュリティ強化の設定 | 151 |
| 信頼できるデバイス | 152 |
| Cisco Unified Communications Manager の管理 | 153 |
| 電話機モデルのサポート | 153 |
| 電話機のセキュリティ設定の表示 | 154 |
| 電話機のセキュリティの設定 | 154 |
| 推奨ベンダーの SIP 電話セキュリティのセットアップ | 155 |
| 推奨ベンダーの SIP 電話セキュリティプロファイルのデバイスごとの証明書の設定 | 155 |
| 推奨ベンダーの 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 | 156 |
| クラスタ間での電話の移行 | 157 |
| 電話セキュリティの連携動作と制限事項 | 158 |
| 電話セキュリティプロファイル | 158 |
| 電話セキュリティプロファイルの設定 | 159 |
| 電話のセキュリティの設定タスクフロー | 174 |

| | |
|--------------------------------------|-----|
| 電話セキュリティプロファイルの検索 | 175 |
| 電話セキュリティプロファイルのセットアップ | 176 |
| 電話機へのセキュリティプロファイルの適用 | 176 |
| 電話機のセキュリティプロファイルと電話機の同期 | 177 |
| 電話セキュリティプロファイルの削除 | 177 |
| 電話機のセキュリティプロファイルを使用した電話機の検索 | 178 |
| SIP トランク セキュリティ プロファイルのインタラクションと制限事項 | 179 |
| SIP 電話機のダイジェスト認証の概要 | 179 |
| SIP 電話機のダイジェスト認証の前提条件 | 179 |
| SIP 電話のダイジェスト認証の設定タスクフロー | 180 |
| 電話ユーザへのダイジェストクレデンシャルの割り当て | 180 |
| 電話セキュリティプロファイルでのダイジェスト認証の有効化 | 181 |
| 電話機へのダイジェスト認証の割り当て | 181 |
| SIP ステーションレルムの設定 | 182 |
| エンドユーザのダイジェストクレデンシャルの設定 | 182 |

第 12 章

| | |
|---|-----|
| セキュアな会議リソースの設定 | 183 |
| セキュアな会議 | 183 |
| 会議ブリッジの要件 | 184 |
| セキュアな会議アイコン | 185 |
| セキュアな会議のステータス | 186 |
| アドホック会議のリスト | 187 |
| 最小セキュリティレベルの会議の開催 | 188 |
| Cisco Unified IP 電話 セキュアな会議とアイコンのサポート | 189 |
| セキュアな会議の CTI サポート | 190 |
| トランクとゲートウェイを介したセキュアな会議 | 190 |
| CDR データ | 190 |
| 連携動作と制限事項 | 190 |
| Cisco Unified Communications Manager のセキュアな会議とのインタラクション | 191 |
| セキュアな会議による Cisco Unified Communications Manager の制約事項 | 192 |
| 会議リソースの保護のヒント | 192 |

| | |
|--|-----|
| セキュアな会議ブリッジのセットアップ | 194 |
| Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定 | 195 |
| ミーティング会議の最小セキュリティ レベルの設定 | 196 |
| セキュアな会議ブリッジのパケット キャプチャの設定 | 196 |

第 13 章

| | |
|------------------------------------|------------|
| ボイス メッセージング ポートのセキュリティ設定 | 199 |
| ボイスメッセージングセキュリティ | 199 |
| ボイスメッセージングセキュリティの設定のヒント | 200 |
| セキュアなボイスメッセージングポートのセットアップ | 201 |
| 単一のボイスメッセージングポートへのセキュリティプロファイルの適用 | 202 |
| ボイスメールポートウィザードを使用したセキュリティプロファイルの適用 | 202 |

第 14 章

| | |
|------------------------|------------|
| セキュアトーンとアイコン | 205 |
| セキュアトーンとアイコンの概要 | 205 |
| セキュアな電話コールの識別 | 207 |
| セキュアアイコンとセキュアトーンのヒント | 208 |
| サポートされるデバイスのセキュアトーン | 209 |
| 保護されたデバイスのセキュアトーン | 209 |
| セキュアアイコンとセキュアトーン設定のタスク | 210 |
| セキュアアイコンポリシーの設定 | 210 |
| クラスタのセキュア通知トーンの有効化 | 211 |
| 電話機の保護デバイスとしての設定 | 212 |
| セキュアコールとセキュアトーンの制限事項 | 212 |

第 15 章

| | |
|---|------------|
| トランクとゲートウェイの SIP セキュリティ | 215 |
| トランクとゲートウェイの SIP セキュリティの概要 | 215 |
| SIP トランクの暗号化 | 215 |
| Cisco IOS MGCP ゲートウェイの暗号化 | 216 |
| H.323 ゲートウェイおよび h.323/h.323/h トランク暗号化 (h.323) | 217 |
| SIP トランク セキュリティ プロファイルの設定について | 219 |
| SIP トランク セキュリティ プロファイルの設定のヒント | 219 |

| | |
|--|-----|
| トランクとゲートウェイの SIP セキュリティ設定タスクフロー | 220 |
| セキュアゲートウェイとトランクのセットアップ | 220 |
| SIP トランク セキュリティプロファイルの設定 | 221 |
| SIP トランク セキュリティプロファイルの設定 | 222 |
| SIP トランクセキュリティプロファイルの適用 | 229 |
| Sip トランクセキュリティプロファイルと SIP トランクの同期 | 230 |
| Cisco Unified Communications Manager Administration を使用した SRTP の許可 | 230 |

 第 16 章

TLS セットアップ 233

| | |
|------------------------------------|-----|
| TLS の概要 | 233 |
| TLS の前提条件 | 233 |
| TLS 設定タスク フロー | 234 |
| 最小 TLS バージョンの設定 | 235 |
| TLS 暗号化の設定 | 235 |
| SIP トランクのセキュリティプロファイルでの TLS の設定 | 236 |
| SIP トランクへのセキュアプロファイルの追加 | 236 |
| 電話セキュリティプロファイルでの TLS の設定 | 237 |
| 電話へのセキュア電話プロファイルの追加 | 238 |
| ユニバーサルデバイス テンプレートへのセキュア電話プロファイルの追加 | 238 |
| TLS の連携動作と制約事項 | 239 |
| TLS の相互作用 | 240 |
| TLS の制限 | 240 |

 第 III 部 :

ユーザセキュリティ 247

 第 17 章

ID の管理 249

| | |
|---------------|-----|
| ユーザセキュリティの概要 | 249 |
| アイデンティティ管理の概要 | 250 |
| SAML SSO の展開 | 251 |
| LDAP 認証 | 252 |
| LDAP 認証の設定 | 252 |

| | |
|-----------------------|-----|
| ローカルデータベース認証 | 253 |
| OAuth フレームワーク | 254 |
| SIP OAuth モードの設定 | 255 |
| 既存の OAuth 更新トークンの取り消し | 255 |

第 18 章**クレデンシャル ポリシー 257**

| | |
|------------------------------------|-----|
| クレデンシャル ポリシーの概要 | 257 |
| クレデンシャル ポリシーの JTAPI および TAPI のサポート | 259 |
| デフォルトのクレデンシャル ポリシーの設定 | 259 |
| エンドユーザログイン情報またはログイン情報ポリシーの編集 | 260 |
| PIN同期の有効化 | 261 |
| 認証アクティビティのモニタ | 262 |
| クレデンシャル キャッシングの設定 | 263 |
| セッションの終了の管理 | 264 |

第 19 章**連絡先検索認証 267**

| | |
|---------------------------|-----|
| 連絡先検索認証の概要 | 267 |
| 連絡先検索認証タスクフロー | 267 |
| 連絡先検索の認証の電話サポートの確認 | 268 |
| 連絡先検索の認証の有効化 | 268 |
| 連絡先検索用のセキュアなディレクトリ サーバの設定 | 268 |

第 IV 部 :**高度なシステムセキュリティ 271**

第 20 章**FIPS モードの設定 273**

| | |
|------------------------|-----|
| FIPS 140-2 の設定 | 273 |
| FIPS 140-2 モードの有効化 | 274 |
| CiscoSSH サポート | 277 |
| FIPS 140-2 モードの無効化 | 278 |
| FIPS 140-2 モードのステータス確認 | 278 |
| FIPS 140-2 モードサーバのリポート | 279 |

| | |
|---------------------|-----|
| FIPS モードの制約事項 | 279 |
| 強化されたセキュリティ モード | 281 |
| 強化されたセキュリティ モードの設定 | 283 |
| コモンクライテリア モード | 284 |
| コモンクライテリア構成のタスク フロー | 284 |
| TLSの有効化 | 285 |
| コモンクライテリア モードの構成 | 286 |

 第 21 章

| | |
|--|------------|
| V.150 の最小必須要件 | 289 |
| V.150 の概要 | 289 |
| V.150 設定のタスク フロー | 289 |
| メディア リソース グループ設定のタスク フロー | 291 |
| 非 V.150 エンドポイントのメディア リソース グループの設定 | 291 |
| 非 V.150 エンドポイントのメディア リソース グループ リストの設定 | 292 |
| V.150 エンドポイントのメディア リソース グループの設定 | 292 |
| V.150 エンドポイントのメディア リソース グループ リストの設定 | 293 |
| Cisco V.150 (MER) に対応したゲートウェイの設定 | 293 |
| V.150 MGCP ゲートウェイ ポート インターフェイスの設定 | 294 |
| V.150 SCCP ゲートウェイ ポート インターフェイスの設定 | 295 |
| 電話での V.150 サポートの設定 | 295 |
| SIP トランク設定のタスク フロー | 296 |
| V.150 の SIP プロファイルの設定 | 296 |
| クラスタ全体の V.150 フィルタの設定 | 297 |
| SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加 | 298 |
| V.150 の SIP トランクの設定 | 298 |

 第 22 章

| | |
|------------------|------------|
| IPSec の設定 | 301 |
| IPsec の概要 | 301 |

 第 23 章

| | |
|--|------------|
| CTI、JTAPI、および TAPI の認証および暗号化の設定 | 303 |
| CTI、JTAPI、および TAPI アプリケーションの認証 | 303 |

| | |
|---|---|
| CTI、JTAPI、および TAPI アプリケーションの暗号化 | 305 |
| CTI ポートの強力な暗号スイート | 306 |
| CTI、JTAPI、および TAPI アプリケーションの CAPF の機能 | 307 |
| CTI、JTAPI、および TAPI アプリケーションの CAPF システムインタラクションと要件 | 308 |
| Certificate Authority Proxy Function サービスのアクティブ化 | 309 |
| アプリケーションユーザまたはエンドユーザの CAPF プロファイルの設定 | 309 |
| CAPF の設定項目 | 310 |
| CAPF サービス パラメータの更新 | 312 |
| 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 プロファイルの削除 | 313 |
| CTI、JTAPI、および TAPI の保護 | 314 |
| セキュリティ関連のアクセス制御グループへのアプリケーションとエンドユーザの追加 | 315 |
| 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 | 317 |
| アプリケーションまたはエンドユーザの証明書の操作ステータスの表示 | 318 |
| <hr/> | |
| 第 24 章 | セキュアな録音とモニタリング 319 |
| | セキュアコールのモニタリングと録音のセットアップについて 319 |
| | セキュアなコールのモニタリングと録音のセットアップ 320 |
| <hr/> | |
| 第 25 章 | VPN クライアント 321 |
| | VPN クライアントの概要 321 |
| | VPN クライアント設定のタスク フロー 321 |
| | Cisco IOS の前提条件の完了 322 |
| | IP 電話をサポートするための Cisco IOS SSL VPN の設定 323 |
| | AnyConnect 用の ASA 前提条件への対応 325 |
| | IP 電話 での VPN クライアント用の ASA の設定 325 |
| | VPN コンセントレータの証明書のアップロード 327 |
| | VPN ゲートウェイの設定 328 |
| | VPN クライアント用 VPN ゲートウェイのフィールド 329 |
| | VPN グループの設定 329 |

| | |
|------------------------------|-----|
| VPN クライアント用 VPN グループのフィールド | 330 |
| VPN プロファイルの設定 | 330 |
| VPN クライアント用 VPN プロファイルのフィールド | 331 |
| VPN 機能のパラメータの設定 | 332 |
| VPN 機能のパラメータ | 332 |
| 共通の電話プロファイルへの VPN の詳細の追加 | 334 |

| | | |
|--------|------------------------|-----|
| 第 26 章 | オペレーティングシステムとセキュリティの強化 | 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 | 341 |
|---------|-------------|-----|

| | | |
|--------|-------------------------|-----|
| 第 27 章 | セキュリティトラブルシューティングの概要 | 343 |
| | リモート アクセス | 343 |
| | Cisco Secure Telnet | 344 |
| | ファイアウォールによる保護 | 344 |
| | Cisco Secure Telnet の設計 | 344 |
| | Cisco Secure Telnet の構造 | 345 |
| | リモート アカウントの設定 | 346 |



はじめに

Cisco Unified Communications Manager システムにセキュリティ対策を実装すると、電話や Unified Communications Manager サーバの個人情報/ID の盗用、データ改ざん、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できます。

CiscoIP テレフォニーネットワークでは、認証済み通信ストリームを確立および維持し、ファイルを電話に転送する前にそのファイルにデジタル署名して、Cisco Unified IP 電話 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 \(xix ページ\)](#)
- [表記法 \(xx ページ\)](#)
- [法令順守 \(xxi ページ\)](#)

このマニュアルについて

このセキュリティガイドには、短い説明を含む次の部分が含まれています。

表 1: 部分と説明

| パート | 説明 |
|----------------|---|
| CUCM セキュリティの概要 | <p>セキュリティの概要に関する次のトピックの情報を提供します。</p> <ul style="list-style-type: none">• システム要件• 一般的なアイコン• ベストプラクティス <p>また、システム内のセキュリティを設定する概要も提供しています。</p> |

| パート | 説明 |
|----------------|--|
| 基本的なシステムセキュリティ | <p>システムで基本的なセキュリティを設定するための次のトピックに関する情報を提供します。</p> <ul style="list-style-type: none">• 証明書• セキュリティモード• 暗号管理• セキュアトーンとアイコン• TFTP 暗号化• 電話機のセキュリティ• トランクとゲートウェイの SIP セキュリティ• TLS セットアップ |
| ユーザセキュリティ | <p>システムでユーザセキュリティを設定するための次のトピックに関する情報を提供します。</p> <ul style="list-style-type: none">• ID の管理<ul style="list-style-type: none">• ユーザアクセス制御• クレデンシャル ポリシー• ディレクトリアクセス<ul style="list-style-type: none">• 連絡先検索認証の設定• 連絡先検索用のセキュアなディレクトリ サーバの設定 |

| パート | 説明 |
|---------------|--|
| 高度なシステムセキュリティ | <p>システムで高度なセキュリティを設定するための次のトピックに関する情報を提供します。</p> <ul style="list-style-type: none">• FIPS モード• 強化されたセキュリティ モード• コモン クライテリア モード• Cisco V.150 最低要件• ECDSA と RSA• IPsec ポリシー• CTI の認証と暗号化の設定• JTAPI、および TAPI• セキュアなコールのモニタリングおよび録音• VPN クライアント |
| 付録 | <p>システムをセキュリティで保護するための次のトピックに関する情報を提供します。</p> <ul style="list-style-type: none">• 追加のセキュリティの設定• 用語および略語• 連携動作と制限事項• Hypertext Transfer Protocol Over Secure Sockets Layer (HTTPS)• 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次のとおりです。

- システム管理者
- 電話管理者

Unified Communications Manager のコールセキュリティ機能を設定します。

表記法

このセクションでは、ガイドに続くドキュメントの表記方法について説明します。

(注) は、次のように表しています。



(注) 重要または追加情報の注釈です。

ヒントは、次のように表しています。



ヒント 役立つ「ヒント」の意味です。

強いレベルの注意は、次のように表しています。



注意 読者は注意する必要がありますという意味です。このような状況では、手順を慎重に読んでください。それ以外の場合、機器に損傷を与えたり、データを失ったりする可能性があります。

弱いレベルの注意は、次のように表しています。



注目 読者は注意を払ってくださいという意味です。このような状況では、手順を慎重に読んでください。それ以外の場合、機器に損傷を与えたり、データを失ったりする可能性があります。

警告



警告 読者は指示に**従わなければならない**という意味です。このような状況では、手順を慎重に読んでください。それ以外の場合、機器に損傷を与えたり、データを失ったりする可能性があります。

法令順守

Unified Communications Manager (セキュリティ) 製品には、暗号化機能とインポート、エクスポート情報が含まれています。情報の転送および使用は、米国および他の国に適用される法律に準拠しています。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意したものと見なされます。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の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。



第 1 章

新機能および変更された機能に関する情報

- [新機能および変更された機能に関する情報, on page 1](#)

新機能および変更された機能に関する情報

次の表は、この最新リリースまでのガイドでの機能の主な変更点の概要を示したものです。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

Table 2: Unified Communications Manager と IM and Presence サービスの新機能と変更された動作

| 日付 | 説明 | 参照先 |
|------------------|---|---|
| 2023 年 12 月 18 日 | IPSec DoDIN APL 認定の StrongSwan サポート | FIPS 140-2 の設定, on page 273 |
| 2023 年 12 月 18 日 | Alma の一部としての FIPS ツールキットの更新 | <ul style="list-style-type: none">• FIPS 140-2 の設定, on page 273• FIPS 140-2 モードの有効化, on page 274 |
| 2023 年 12 月 18 日 | 更新トークンの自動更新のサポート | OAuth フレームワーク, on page 254 |
| 2023 年 12 月 18 日 | Oauth : CUCM パブリッシャに対する更新トークンの依存関係を排除します。 | 『 Cisco Unified Communications Manager システム設定ガイド 』の「共通エンタープライズパラメータ」セクションを参照してください。 |

| 日付 | 説明 | 参照先 |
|------------------|------------------------------------|---|
| 2023 年 12 月 18 日 | 証明書失効リストのサポート | 証明書失効の設定, on page 75 『Cisco Unified Communications Manager システム設定ガイド』の「共通エンタープライズパラメータ」セクションを参照してください。 |
| 2023 年 12 月 18 日 | Cisco SSL6 から Cisco SSL7 へのアップグレード | FIPS 140-2 の設定, on page 273 |



第 1 部

Unified CM のセキュリティの概要

- [概要 \(5 ページ\)](#)
- [コンフィギュレーション \(11 ページ\)](#)
- [デフォルトのセキュリティ \(15 ページ\)](#)



第 2 章

概要

- システム要件 (5 ページ)
- ベストプラクティス (5 ページ)
- 一般的なアイコン (8 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を次に示します。

- Unified Communications Manager パブリッシャの Cisco Unified Communications Manager Administration 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。
- Unified Communications Manager で TLS 接続を認証するために、すべての電話機にローカルで有効な証明書（LSC）が存在します。



(注) LSCが存在しない場合は、一部のエンドポイントでもMICが使用されますが、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

シスコでは、次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導入する前に、安全なラボ環境でインストールと設定のタスクを常に実行してください。
- リモートロケーションにあるゲートウェイおよびその他のアプリケーションサーバにIPSecを使用します。



警告 これらのインスタンスで IPsec を使用しないと、セッション暗号キーが暗号化されずに転送されます。

- 電話料金の詐欺行為の防止するため、『[Cisco Unified Communications Manager システム設定ガイド](#)』で説明されている電話会議の機能拡張を設定します。同様に、コールの外部転送を制限する設定作業を実行することもできます。この作業の実行方法については、『[Cisco Unified Communications Manager 機能設定ガイド](#)』を参照してください。

デバイスのリセット、サーバとクラスタのリポート、およびサービスの再起動

次の表に、リセット、再起動、およびリポートの詳細を含むセキュリティアクションを示します。

表 3: リセット、再起動、およびリポートを含むセキュリティアクションの詳細:

| シリアル番号 | 操作 | リセット (あり/なし) | 再起動 (あり/なし) |
|--------|----------------------|--------------|---|
| 1 | セキュリティプロファイルの適用 | ○ | いいえ |
| 2 | 電話機のセキュリティ強化の適用 | — | — |
| 3 | セキュリティモードの変更 | ありすべてのデバイス | あり CallManager サービスを再起動します。 |
| 4 | CTL ファイルの更新 | — | はい。すべての暗号化および認証された電話機は、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 接続のポートの更新 | — | あり CTL プロバイダーサービスを再起動します。 |
| 6 | CAPF サービスパラメータの更新/設定 | — | あり シスコ認証局プロキシ機能サービスの再起動 |

| シリアル番号 | 操作 | リセット (あり/なし) | 再起動 (あり/なし) |
|--------|--|---------------|---|
| 7 | CTLプロバイダーサービスの開始または停止 | — | ありすべての Cisco CallManager サービスおよび Cisco TFTP サービスを再起動します。 |
| 7 | セキュアな SRST リファレンスの設定 | あり従属デバイスのリセット | — |
| 8 | スマートカードサービスを開始および自動に変更 | — | はい |
| 9 | アプリケーションユーザの CAPF プロファイルに関連付けられているセキュリティ関連サービスパラメータを設定します。 | — | ありその後、Cisco IP Manager Assistant サービス、Cisco Web Dialer Web サービス、および Cisco Extended Functions サービスを再起動します。 |

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。

電話の設定を更新した後に単一のデバイスをリセットするには、[電話セキュリティプロファイル](#)の適用に関連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、およびサービスのリセット

このセクションでは、Cisco Unified Serviceability で、デバイス、サーバ、クラスタ、およびサービスをリセットするシナリオについて説明します。

クラスタ内のすべてのデバイスをリセットするには、次の手順を実行します。

ステップ 1 Unified Communications Manager から、[システム (System)] > [CiscoUnifiedCM] を選択します。

ステップ 2 [検索 (Find)] をクリックします。

設定されている Unified Communications Manager サーバのリストが表示されます。

ステップ 3 デバイスをリセットする 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 クラスタ内のサーバごとにステップ 2 とステップ 4 を実行します。

割り込みセットアップによるメディア暗号化

暗号化用に Cisco Unified IP Phone 7962 および 7942 の割り込みを設定し、Cisco Unified Communications Manager Administration で次のタスクを実行します。

- CLI コマンド (utils ctl set cluster mixed-mode) を使用してクラスターセキュリティモードを更新します。
- [サービスパラメータ (Service Parameter)] ウィンドウで、[有効な組み込みブリッジ (Builtin Bridge Enable)] パラメータを更新します。

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 Phone モデル 7962 および 7942 の暗号化を設定する場合、暗号化されたデバイスは、暗号化されたコールに参加しているときに割り込みリクエスト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と、割り込みの試行は失敗します。

Cisco Unified IP Phone 7962 および 7942 (暗号化されたセキュリティプロファイルで設定済み) では、[電話の設定 (Phone Configuration)] ウィンドウにメッセージが表示されません。[組み込みブリッジ (Built In Bridge)] 設定に [デフォルト (Default)] を選択するか、または [Default] と同等のデフォルト設定を選択します。いずれの選択にも同じ制限が適用されます。



ヒント 変更を有効にするには、依存する Cisco IP デバイスをリセットする必要があります。

一般的なアイコン

Unified Communications Manager は、コールに参加するサーバおよびデバイスのセキュリティレベルに応じてコール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機に、コールのセキュリティレベルが表示されます。

- シグナリングセキュリティレベルが認証済みのコールに対して、保護アイコンが表示されます。シールドは、Cisco IP デバイス間のセキュリティで保護された接続を識別します。つまり、デバイスは認証済みで、暗号化済みのシグナリングを使用していることを意味します。
- 暗号化されたメディアを使用するコール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) 一部の電話機モデルでは、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、クラスタ間、クラスタ間、およびマルチホップコールで変更できます。SCCP 回線、SIP 回線、および h.323 シグナリングは、参加しているエンドポイントに対するコールセキュリティステータスの変更に関する通知をサポートします。

音声コールとビデオコールは、コールセキュリティステータスのベースとなります。音声とビデオの両方がセキュアである場合に限り、安全とみなされます。



-
- (注) 「Override BFCP Application Encryption Status When Designating Call Security Status」 サービスパラメータは、パラメータ値が [True] で音声セキュアであると、ロックアイコンを表示します。この状態は、他のすべてのメディアチャネルのセキュリティステータスを無視します。デフォルトパラメータ値は [False] です。
-

会議および割り込みコールの場合、[セキュリティ (security)] アイコンに会議のセキュリティステータスが表示されます。



第 3 章

コンフィギュレーション

- [セキュリティの設定 \(11 ページ\)](#)

セキュリティの設定

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と、さまざまなセキュリティタスクフローおよびその簡単な説明への参照を提供します。

表 4: セキュリティの設定

| 手順 | 手順 | 説明 |
|--------|----------------------|--|
| ステップ 1 | 証明書の生成 | システムの証明書を設定および交換します。 |
| ステップ 2 | 証明書のモニタリングと失効の設定 | システムを設定して、証明書の期限をモニタし、オンライン証明書ステータスプロトコル (OCSP) を介して証明書を自動的に失効させます。 |
| ステップ 3 | 混合モードの有効化 | 混合モードが有効になっている場合、Cisco Unified IP Phone、TelePresence エンドポイント、または OAuth なしで Jabber を導入する場合、システムはセキュリティに証明書信頼リスト (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) の設定 | CAPF を設定して、電話機の LSC 証明書を生成します。 |
| ステップ 5 | 暗号化された TFTP の設定 | 電話機に送信された最初の電話機設定ファイルが暗号化される、暗号化された TFTP を設定します。 |
| ステップ 6 | 電話機のセキュリティの設定 | 電話機の TFTP 暗号化や TLS シグナリングなどの項目を含めるには、電話機のセキュリティプロファイルを設定します。 |

| 手順 | 手順 | 説明 |
|---------|------------------------------------|--|
| ステップ 7 | 電話のセキュリティ強化の設定 | 電話機への接続のセキュリティを強化するために、オプションの製品固有の設定を行います。 |
| ステップ 8 | セキュアトランクの設定 | セキュア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 | トランクでの SIP の有効化 | SRTP に対して SIP トランクを設定します。 |
| ステップ 10 | [SAML SSO の有効化 (Enable SAML SSO)] | アイデンティティ管理フレームワークを設定します。 アイデンティティ管理には、SAML SSO をお勧めします。ただし、LDAP 認証またはローカル認証も使用できます。 |
| ステップ 11 | ユーザ アクセスの設定 | エンドユーザを、必要なロールとアクセス権限を含むアクセス制御グループに割り当てます。 |
| ステップ 12 | クレデンシャルポリシーの設定 | ユーザパスワード、ユーザ PIN、アプリケーションユーザパスワードのなどのデフォルトログイン情報ポリシーを設定します。 |
| ステップ 13 | 連絡先検索の認証の設定 | すべてのディレクトリ検索を認証して、会社のディレクトリを保護します。 |
| ステップ 14 | TLS の有効化 | 電話機の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使用して 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暗号のリストをカスタマイズします。 |
| ステップ 16 | IPsec ポリシーの設定 | システムの 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 のセキュリティ強化の設定 | OS のセキュリティ強化を設定します。 |
| ステップ 19 | FIPS の設定 | FIPS モード、強化されたセキュリティモード、およびコモンクライテリアモードを設定し、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のガイドラインを満たします。 |

| 手順 | 手順 | 説明 |
|---------|-------------|---|
| ステップ 20 | セキュリティ機能の設定 | <p>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。</p> <ul style="list-style-type: none">• セキュアなモニタリングとレコーディング• セキュア会議• セキュアトーンとアイコン• V.150• モバイル & リモート アクセス• AS-SIP |



第 4 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 \(15 ページ\)](#)
- [暗号化 \(26 ページ\)](#)
- [デフォルトのセキュリティ管理タスク \(37 ページ\)](#)

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、追加の設定要件なしでサポートされる Cisco Unified IP Phone の基本的なレベルのセキュリティを提供します。

この機能は、サポートされる IP 電話機に対して次のデフォルトの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、次のコンポーネントを使用して非セキュアな環境で基本的なセキュリティを提供します。

- アイデンティティ信頼リスト (ITL) : このファイルは、クラスタのインストール時に TFTP サービスがアクティブ化された後、信頼の確立のために Cisco Unified IP Phone 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 Phone の証明書を認証します。TVS 証明書と他のいくつかのキー証明書が ITL ファイルにバンドルされます。

初期信頼リスト

初期信頼リスト (ITL) ファイルは、エンドポイントが Unified Communications Manager を信頼できるように、最初のセキュリティに使用されます。ITL は明示的に有効にするセキュリティ機能を必要としません。ITL ファイルは、TFTP サービスがアクティブになり、クラスタがイン

ストールされると自動的に作成されます。Unified Communications Manager の TFTP サーバの秘密キーは、ITL ファイルの署名に使用されます。

Unified Communications Manager クラスタまたはサーバが非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 Phone ごと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 ファイルの内容を表示できます。

Cisco Unified IP Phone は、次のタスクを実行するために ITL ファイルが必要です。

- CAPF とセキュアに通信する。設定ファイル暗号化をサポートするための前提条件です。
- 設定ファイルの署名を認証する。
- TVS を使用する 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 CTL ファイルがまだ存在していない場合、最初の ITL ファイルが自動的に信頼されます。テレビは、署名者に対応する証明書を返すことができる必要があります。

Cisco IP 電話に既存の CTL ファイルがある場合、ITL ファイルの署名の認証にその CTL ファイルが使用されます。



-
- (注) SHA-1 または MD5 アルゴリズム値は、初期信頼リスト (ITL) ファイルの値に変更があっ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すると、Cisco IP 電話と Unified Communications Manager クラスタの間にある ITL ファイルの差異を特定できます。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。
-

最初の信頼リスト (ITL) ファイルは、CTL ファイルと同じ形式になっています。ただし、これはより小さく、スリムのバージョンです。

ITL ファイルには次の属性が適用されます。

- TFTP サービスがアクティブ化され、クラスタをインストールすると、システムによって ITL ファイルが自動的に作成されます。内容が変更された場合、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。このファイルはソフト eToken (TFTP サーバの CallManager 証明書に関連付けられている秘密キー) を使用します。
- 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、Cisco Unified IP Phone は 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ています。

- 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：この証明書を使用すると、ITL ファイル署名と電話機設定ファイル署名を認証できます。
- クラスタ上で使用可能なすべての TVS 証明書：これらの証明書を使用すると、電話機は TVS と安全に通信し、証明書認証を要求できます。

- CAPF 証明書: これらの証明書は、コンフィギュレーションファイルの暗号化をサポートします。CAPF 証明書は必ずしも ITL ファイル内に存在する必要はありません (TVS で認証可能) が、CAPF 証明書によって CAPF への接続が簡易化されます。

ITL ファイルには証明書ごとに 1 つのレコードが含まれます。各レコードの内容は次のとおりです。

- 証明書
- Cisco IP 電話によるルックアップを容易にするための、事前に抽出された証明書フィールド。
- 証明書の権限 (TFTP、CUCM、TFTP+CCM、CAPF、TV、SAST)

TFTP サーバの CallManager 証明書は、2 つの異なる権限を持つ次の 2 つの ITL レコード内に存在します。

- TFTP 権限 または TFTP および CCM 権限: 設定ファイルの署名を認証する。
- SAST 権限: ITL ファイルの署名を認証する。

ITLRecovery 証明書の証明書管理の変更

- ITLRecovery の有効期間が 5 年間から 20 年間に延長され、より長い期間にわたって同じ ITLRecovery 証明書が使用されるようになりました。



(注) ITLRecovery 証明書のデフォルトの有効期間は 5 年です。ただし、ITLRecovery 証明書の有効期間を 5、10、15、または 20 年に設定することもできます。Unified Communications Manager のアップグレード時に、新しいリリースに ITLRecovery 証明書がコピーされます。

- 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、トークンレス CTL を使用しており、CallManager 証明書を再生成する場合に、CTL ファイルに更新された CallManager 証明書があり、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。

ITLRecovery 証明書

ITLRecovery Certificate 機能では、新しい **ITL ファイルステータス** ドロップダウンリストが導入され、管理者は古い ITL を持つ電話機を識別して、それらの電話機に必要なアクションを実行できるようになりました。

一部の電話機は、ITL ファイルが更新されたときに最新の ITL ファイルを取得せず、古いものを保持します (CM 証明書の更新など)。システムは、不一致の ITL ファイルがある電話機の集中型レポートをユーザインターフェイスに表示します。

次に、さまざまな ITLRecovery シナリオを示します。

TFTP Service Activaton :

- TFTP サービスがアクティブになると、生成された ITL ファイルのハッシュがサーバのホスト名とともに DB に保存されます。ITL が TFTP コードで更新されるたびに更新されません。
- TFTP ホスト名がすでにテーブルに存在する場合は、生成された ITL ハッシュが保存されている値と比較されます。
 - ITL ハッシュが同じでない場合、新しい ITL ハッシュが DB で更新されます。
 - ITL ハッシュが同じ場合、TFTP ログに「Tftp Itl hash not changed」と表示されます。

デバイス登録と ITLFile のダウンロード

- 電話機が Unified Communications Manager に登録されると、サーバに存在する ITLFile の詳細（サーバのホスト名、ハッシュ、タイムスタンプ）が DB に存在しません。
- 電話機が Unified Communications Manager に登録されると、電話機に適用された ITL ファイルの詳細を含む SIP アラームが送信されます。これは、DB に保存されている ITL ファイルのハッシュと比較されます。
 - ITL ハッシュが同じ場合、デバイスハッシュ情報は新しいタイムスタンプで更新されます。
 - ITL ハッシュが同じでない場合、報告された ITL ハッシュとタイムスタンプがデバイスに対して更新されます。
- 電話機の登録が解除されると、そのデバイスの信頼ハッシュ情報が削除されます。

連携動作と制限事項

Unified Communications Manager クラスタに 39 を超える証明書がある場合、Cisco IP 電話上の ITL ファイルサイズが 64 キロバイトを超えます。ITL ファイルサイズが増加すると、電話での ITL の正常なロードに影響し、Unified Communications Manager での電話登録が失敗することになります。

信頼検証サービス

ネットワーク内に多数の電話機があり、Cisco Unified IP Phone のメモリも限られています。したがって、Unified Communications Manager は TVS を介してリモート信頼ストアとして動作するため、各電話機に証明書信頼ストアを配置する必要はありません。Cisco Unified IP Phone は CTL ファイルまたは ITL ファイルを使用して署名または証明書を検証できないため、検証のために TVS サーバに問い合わせることもできます。したがって、中央信頼ストアを持つことは、信頼ストアをすべての Cisco Unified IP Phone に持つよりも管理が簡単です。

TVS を使用すると、HTTPS を確立しているときに、Cisco Unified IP Phone で EM サービス、ディレクトリ、および MIDlet などのアプリケーションサーバを認証できます。

TV には、次の機能があります。

- 拡張性：Cisco Unified IP Phone 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デフォルトのインストールに含まれており、ユーザの介入は必要ではありません。



(注) セキュアなシグナリングおよびメディアを有効にする場合は、CTL ファイルを作成してから、クラスタを混合モードに設定する必要があります。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 mixed-mode` を使用します。

TVS を説明する基本的な概念を次に示します。

- TVS は、Unified Communications Manager サーバ上で実行され、Cisco IP 電話に代わって証明書を認証します。
- Cisco Unified IP Phone は、信頼できる証明書をすべてダウンロードするのではなく、TVS を信頼する必要があるだけです。
- 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 Phone によりダウンロードされ、信頼はそこからフローします。

認証、整合性、および許可

整合性と認証は、次の脅威から保護します。

- TFTP ファイルの操作 (整合性)
- 電話と Unified Communications Manager との間で行われる呼処理シグナリングの変更 (認証)
- 頭字語で定義している中間者攻撃 (認証)
- 電話およびサーバの ID 盗難 (認証)
- リプレイ アタック (ダイジェスト認証)

認可は、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。1つのセッションで複数の認証方式と許可方式を実装できます。

イメージ認証

このプロセスでは、電話機にロードする前に、ファームウェアロードのバイナリイメージの改ざんを防止します。イメージが改ざんされると、電話の認証プロセスが失敗し、イメージは拒否されます。イメージ認証は、Unified Communications Manager インストール時に自動的にイン

ストールされた署名付きバイナリファイルを使用して実行されます。同様に、web からダウンロードしたファームウェアアップデートにも、署名付きバイナリイメージが提供されます。

デバイス認証

このプロセスは、通信デバイスのアイデンティティを検証し、エンティティが正当なものであることを確認します。

デバイス認証は、Unified Communications Manager サーバと、サポート対象の Cisco Unified IP 電話、SIP トランク、または JTAPI/TAPI/CTI アプリケーション（サポートされている場合）との間で発生します。これらのエンティティ間での認証済み接続は、それぞれのエンティティが相手側エンティティの証明書を受け入れた場合にのみ発生します。相互認証では、相互証明書交換のこのプロセスについて説明します。

デバイス認証は、CiscoCTL ファイルの作成（Unified Communications Manager サーバノードとアプリケーションの認証時）、および Certificate Authority Proxy Function（電話と JTAPI/TAPI/CTI アプリケーションの認証時）に依存します。



ヒント SIP トランク経由で接続される SIP ユーザは、CallManager 信頼ストアに SIP ユーザ エージェント証明書が含まれ、SIP ユーザ エージェントの信頼ストアに Cisco Unified Communications Manager 証明書が含まれる場合に、Cisco Unified Communications Manager で認証されます。CallManager 信頼ストアの更新の詳細については、この Unified Communications Manager リリースに対応した『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。

ファイル認証

このプロセスは、電話機がダウンロードする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、リングリスト、ロケール、および CTL ファイルなどです。ファイルが作成後に改ざんされていないことを確認するため、電話によって署名が検証されます。サポートされるデバイスの一覧については、「電話モデルのサポート」を参照してください。

クラスタを混合モードに設定すると、TFTP サーバは、呼出音リスト、ローカライズされた ca.cnf、およびリングリスト wav ファイル (sgn 形式) などの静的ファイルに署名します。Tftp サーバは、ファイルに対してデータの変更が発生したことを確認するたびに、<デバイス名> 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 サーバは署名されたファイルをディスクに書き込みます。保存されたファイルが変更されたことを TFTP サーバが確認すると、TFTP サーバはファイルを再署名します。ディスク上の新しいファイルは、削除された保存済みファイルを上書きします。電話が新しいファイルをダウンロードできるようになる前に、関連するデバイスを管理者が [Unified Communications Manager] で再起動する必要があります。

電話機は、TFTP サーバからファイルを受信すると、ファイルの署名を検証することによってファイルの整合性を検証します。電話機で認証済み接続を確立するには、次の基準が満たされていることを確認します。

- 証明書が電話内に存在していること。
- CTL ファイルが電話に存在し、そのファイルに Unified Communications Manager エントリと証明書が存在していること。
- 認証または暗号化のためにデバイスを設定しました。

シグナリング認証

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、伝送中にシグナリング パケットが改ざんされ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ます。

ダイジェスト認証

SIP トランクと電話のこのプロセスによって、Unified Communications Manager が Unified Communications Manager に接続されるデバイスのアイデンティティに対するチャレンジを実行できます。チャレンジが実施されると、デバイスはユーザ名とパスワードに類似したダイジェスト クレデンシャルを検証用に Unified Communications Manager に提出します。提出されたクレデンシャルが、データベース内でそのデバイスに対して設定されているクレデンシャルと一致した場合、ダイジェスト認証は成功となり、Unified Communications Manager によって SIP 要求が処理されます。



(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、デバイスには一意のダイジェストユーザ ID とパスワードを登録する必要があります。

電話ユーザやアプリケーション ユーザには、Unified Communications Manager データベースで SIP ダイジェスト クレデンシャルを設定します。

- アプリケーションの場合は、[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウでダイジェストクレデンシャルを指定します。
- SIP を実行している電話の場合は、[エンドユーザ (End User)] ウィンドウでダイジェスト認証クレデンシャルを指定します。ユーザを設定した後にクレデンシャルを電話に関連付けるには、[電話の設定 (Phone Configuration)] ウィンドウでダイジェストユーザ (エンドユーザ) を選択します。電話をリセットした後、ログイン情報は TFTP サーバから電話機に提供される電話設定ファイル内に存在します。TFTP ダウンロードでダイジェストクレデンシャルがクリアテキスト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設定に関連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課題については、SIP レルムを設定します。これにより、レルムのユーザ名(デバイスまたはアプリケーションユーザ)とダイジェストクレデンシャルが指定されます。

外部電話やSIP実行中のトランクに対するダイジェスト認証を有効化してダイジェストクレデンシャルを設定する場合、Unified Communications Manager によってユーザ名、パスワード、レルムのハッシュを含むクレデンシャルのチェックサムが計算されます。システムでは、MD5 ハッシュの計算に、乱数であるナンス値が使用されます。値は Unified Communications Manager によって暗号化され、ユーザ名とチェックサムがデータベースに保存されます。

チャレンジを開始するために、Unified Communications Manager では SIP 401 (Unauthorized) メッセージが使用されます。このメッセージのヘッダーにはナンスとレルムが含まれています。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、nonce の有効期間を設定します。Nonce の有効期間は、nonce 値が有効なままになる分数を指定します。この時間が経過すると、その外部デバイスは Unified Communications Manager によって拒否され、新しい番号が生成されます。



- (注) Unified Communications Manager は SIP トランク経由で着信した、回線側の電話やデバイスから発信された SIP コールに対してはユーザエージェントサーバ (UAS) として動作し、SIP トランクに由来する SIP コールに対してはユーザエージェントクライアント (UAC) として動作し、回線から回線へ、またはトランクからトランクへの接続に対してはバックツーバックユーザエージェント (B2BUA) として動作します。ほとんどの環境において、Unified Communications Manager は主に SCCP と SIP エンドポイントを接続する B2BUA として動作します。(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 ダイジェスト認証では、整合性や機密性は提供されません。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は、デバイスの TLS プロトコルを設定します。デバイスが暗号化をサポートしている場合は、デバイスセキュリティモードを暗号化として設定します。デバイスが暗号化された電話設定ファイルをサポートしている場合は、ファイルの暗号化を設定します。

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化すると、キープアライブメッセージを除き、SIP を実行中の電話に対するすべての要求に対して Unified Communications Manager はチャレンジを実施します。Unified Communications Manager は回線側電話からのチャレンジに応答しません。

応答を受信すると、Unified Communications Manager はデータベースに保存されたユーザ名のチェックサムを、応答ヘッダー内のクレデンシャルに対して検証します。

SIP を実行中の電話は Unified Communications Manager レルムに存在します。このレルムはインストール時に [Unified Communications Manager Administration] で定義されます。SIP レルムは、サービスパラメータ [SIP Station Realm] を使用して電話にチャレンジするように設定します。

各ダイジェストユーザは、レルムごとに1セットのダイジェストクレデンシャル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も、ダイジェストクレデンシャルを設定しない場合、電話機は登録に失敗します。クラスタモードが非セキュアであり、かつダイジェスト認証が有効化されダイジェストクレデンシャルが設定されている場合、ダイジェストクレデンシャルが電話に送信され、Unified Communications Manager は依然として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化すると、Unified Communications Manager は、SIP トランクを介して接続された SIP デバイスとアプリケーションからの SIP トランク要求に対してチャレンジを実施します。システムでは、チャレンジメッセージ内で [Cluster ID] エンタープライズパラメータが使用されます。SIP トランクを介して接続する SIP ユーザエージェントは、[Unified Communications Manager] でデバイスまたはアプリケーションに設定された一意のダイジェストクレデンシャルを使用して応答します。

Unified Communications Manager が SIP トランク要求を開始した場合、SIP トランクを介して接続された SIP ユーザエージェントは Unified Communications Manager のアイデンティティにチャレンジを行えます。これらの着信チャレンジに対しては、要求されたクレデンシャルをユーザに提供するように SIP レルムを設定します。Unified Communications Manager が SIP 401

(Unauthorized) または SIP 407 (Proxy Authentication Required) メッセージを受信した場合、Unified Communications Manager はトランクを介して接続するレルムの暗号化パスワードおよびチャレンジメッセージに指定されているユーザ名の暗号化されたパスワードをロックアップします。Unified Communications Manager によってパスワードが復号され、ダイジェストが計算され、応答メッセージ内に表現されます。



ヒント レルムは、SIP トランクを介して接続するドメイン (xyz.com など) を表します。これは、要求の送信元を識別するのに役に立ちます。

SIP レルムを設定するには、SIP トランクのダイジェスト認証に関連するトピックを参照してください。Unified Communications Manager にチャレンジを行うことができる SIP トランク ユーザエージェントごとに、Unified Communications Manager で SIP レルム、ユーザ名、パスワードを設定する必要があります。各ユーザエージェントは、レルムごとに1セットのダイジェストクレデンシャルを持つことができます。

認証

Unified Communications Manager では、許可プロセスを使用して、SIP が実行されている電話、SIP トランク、および SIP トランクの SIP アプリケーション要求からのメッセージについて、特定のカテゴリを制限します。

- SIP INVITE メッセージと in-dialog メッセージ、および SIP が実行されている電話の場合、Unified Communications Manager では、コーリング サーチ スペースおよびパーティションによって許可を与えます。
- 電話機からの SIP SUBSCRIBE 要求の場合、Unified Communications Manager では、プレゼンスグループへのユーザアクセスに許可を与えます。
- SIP トランクの場合、Unified Communications Manager では、プレゼンス サブスクリプションおよび特定の非 INVITE SIP メッセージ (Out-of-Dialog REFER、Unsolicited NOTIFY、Replaces ヘッダー付き SIP 要求など) の許可を与えます。許可された SIP 要求をウィンドウで確認する場合は、[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)] ウィンドウで承認を指定します。

SIP トランクアプリケーションの許可を有効にするには、[SIP Trunk Security Profile] ウィンドウで [Enable Application Level Authorization] チェックボックスと [Digest Authentication] チェックボックスをオンにします。次に、[Application User Configuration] ウィンドウで [allowed SIP request] 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イネーブルにすると、最初に sip トランクに対して認証が行われ、次に SIP アプリケーションユーザに対して許可が行われます。トランクの場合、Unified Communications Manager では、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 情報は、着信 SIP 要求に適用されます。ACL で SIP 要求が許可されていない場合、コールは 403 禁止メッセージで失敗します。

ACL で SIP 要求が許可されている場合、Unified Communications Manager では、[SIP Trunk Security Profile] 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。ダイジェスト認証が無効でアプリケーションレベルの認証も無効の場合、Unified Communications Manager では要求を処理します。ダイジェスト認証が有効な場合、Unified Communications Manager では、着信要求に認証ヘッダーが存在することを確認してから、ダイジェスト認証を使用して発信元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 では 401 メッセージでデバイスに対するチャレンジを行います。

アプリケーションレベルの ACL を適用する前に、Unified Communications Manager では、ダイジェスト認証で SIP トランクユーザエージェントを認証します。したがって、アプリケーションレベルの認証を実行するには、その前に、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する必要があります。

NMAP スキャン操作

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して、脆弱性スキャンを実行できます。NMAP は、ネットワーク調査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を表します。



(注) NMAP DP スキャンが完了するまでに最大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>
```

定義：

-n：DNS 解決なし。検出されたアクティブ IP アドレスに対して逆引き DNS 解決を行わないよう NMAP に指示します。NMAP 組み込みパラレルスタブリゾルバを使用しても DNS の処理は遅くなる可能性があるため、このオプションを使用するとスキャン時間を削減できます。

-v：冗長性レベルを上げます。これにより、進行中のスキャンに関する詳細情報が NMAP によって出力されます。開いているポートが検出されると、システムは開いているポートを表示します。NMAP がスキャンに数分以上かかると推定した場合は、完了時間の推定値を提供します。このオプションは、冗長性をさらに高めるために2回以上使用してください。

-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。個々のポート番号は、ハイフンで区切られた範囲であることに注意してください(たとえば、1-1023)。

ccm_ip_address：Cisco Unified Communications Manager の IP アドレス。

自動登録

システムは混合モードと非セキュアモードの両方で自動登録をサポートします。また、デフォルトの設定ファイルに対する署名も行われます。「デフォルトのセキュリティ」がサポートされていない Cisco IP 電話には、署名されていないデフォルトの設定ファイルが提供されます。

Cisco Unified Communications Manager と ITL ファイルを使用したクラスタ間での IP フォンの移行

Unified Communications Manager 8.0(1) 以降では、新しいデフォルトのセキュリティ機能と初期信頼リスト (ITL) ファイルが導入されました。この新機能を使用する場合は、異なるユニファイド CM クラスタ間で電話を移動する際には注意が必要です。また、移行のための適切な手順に従っていることを確認してください。



注意 正しい手順に従わないと、数千台の電話の ITL ファイルを手動で削除しなければならない状況が発生する可能性があります。

新しい ITL ファイルをサポートする Cisco IP 電話では、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 ファイルが電話にインストールされると、設定ファイルおよび ITL ファイルの以降の更新では、以下のいずれかによる署名が必要となります。

- 電話機に現在インストールされている TFTP サーバ証明書
- クラスタのいずれかで TV サービスを検証できる TFTP 証明書。ITL ファイルにリストされているクラスタ内の TV サービスの証明書を確認できます。

この新しいセキュリティ機能により、電話を別のクラスタに移動する場合に、次の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 ファイルが現在の ITL ファイルの署名者によって署名されていないため、電話が新しい ITL ファイルや設定ファイルを受け入れることができない問題。
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すると接続できなくなる可能性があるという問題。
3. TVS サーバが証明書の検証のためにアクセス可能でも、古いクラスタサーバには新しいサーバ証明書がない可能性があるという問題。

この3つの問題のうち1つ以上が発生した場合、考えられる解決策の1つは、クラスタ間を移動中のすべての電話から ITL ファイルを手作業で削除することです。ただし、この解決方法は電話の数が増えるにつれて大変な労力を必要とするため、望ましい解決策ではありません。

最も推奨されるオプションは、Cisco Unified CM エンタープライズ パラメータ [Prepare Cluster for Rollback to pre-8.0] を使用することです。このパラメータを [True] に設定すると、電話は空の TVS および TFTP 証明書セクションを含む特殊な ITL ファイルをダウンロードします。

電話に空の ITL ファイルがあると、(8.x 以前の Unified CM クラスタへの移行の場合) 電話は署名のない設定ファイルをすべて受け入れます。また、(異なる Unified CM 8.x クラスタへの移行の場合) 新しい ITL ファイルをすべて受け入れます。

空の ITL ファイルは、電話の [Settings] > [Security] > [Trust List] > [ITL] をチェックすることで確認できます。古い TVS や TFTP サーバが指定されていた場所には、空のエントリが表示されます。

新しい空の ITL ファイルをダウンロードできるまで、電話には古い 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する予定の場合は、[Prepare cluster For Rollback to pre-8.0] エンタープライズパラメータを無効にして、デフォルトでセキュリティを復元します。

暗号化



ヒント 暗号化機能は、Unified Communications Manager をサーバ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。

ここでは、Unified Communications Manager のサポートする暗号化のタイプについて説明します。

セキュア エンド ユーザ ログイン クレデンシャル

Unified Communications Manager リリース 12.5(1) 以降、すべてのエンドユーザ ログイン クレデンシャルは、強化されたセキュリティを提供するために SHA2 を使用してハッシュされています。

ます。Unified Communications Manager リリース 12.5(1) 以前は、エンドユーザのログインクレデンシャルは、SHA1 のみを使用してハッシュされていました。Unified Communications Manager リリース 12.5(1) には「古いクレデンシャルのアルゴリズムを持つユーザの Unified CM」レポートも含まれます。このレポートは、Cisco Unified Reporting のページで入手できます。このレポートを使用すると、管理者は、パスワードまたは PIN が SHA1 でハッシュされているすべてのエンドユーザをリストできます。

SHA1 でハッシュされているエンドユーザのすべてのパスワードまたは PIN は、最初にログインが成功したときに自動的に SHA2 に移行されます。SHA1 でハッシュされている（古い）クレデンシャルを持つエンドユーザは、次のいずれかの方法を使用して、自身の PIN またはパスワードを更新できます。

- 電話機のエクステンション モビリティまたはディレクトリの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。

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

シグナリング暗号化

シグナリング暗号化により、デバイスと Unified Communications Manager サーバ間で送信されるすべての SIP と SCCP シグナリング メッセージが暗号化されるようになります。

シグナリング暗号化によって、相手に関連する情報、相手が入力した DTMF 番号、コールステータス、メディア暗号キーなどの情報が、意図しないアクセスや不正なアクセスから保護されます。

クラスタを混合モードに設定している場合、Unified Communications Manager によるネットワーク アドレス変換 (NAT) はサポートされません。NAT はシグナリング暗号化では動作しません。

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のファイアウォールトラバース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できる側のメディアソースが、ファイアウォールを介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過する双方向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できないため、ファイアウォールの外側に存在する必要があります。

シグナリング暗号化は、NAT トラバース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

セキュアリアルタイムプロトコル (SRTP) を使用するメディア暗号化により、目的の受信者だけがサポートされているデバイス間で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のマスターキーペアの作成、デバイスへのキー配布、キーが転送される間のキー配布の保護などが含まれます。Unified Communications Manager では、SIP トランクに加えて、主に IOS ゲートウェイと、ゲートキーパー制御および非ゲートキーパー制御トランクの Unified Communications Manager H.323 トランク向けに SRTP がサポートされています。



- (注) Cisco Unified Communications Manager では、デバイスおよびプロトコルの違いに応じて異なる方法でメディア暗号化キーが処理されます。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。この場合、TLS 暗号化シグナリングチャンネルによっ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、それ自体のメディア暗号化キーを生成して保存します。Unified Communications Manager システムによって導出されたメディア暗号化キーは、暗号化されたシグナリングパス経由で、H.323 用の IPsec で保護されたリンク、および SCCP と SIP 向けの MGCP または暗号化 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 を使用できる場合、ネゴシエーション時にステータスを示す必要があります。デバイスがキャッシュされた以前のネゴシエーション SDP を同じコール内の異なるデバイスと使用する場合、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。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、トランスコーディング、保留音などの場合に発生する可能性があります。

セキュリティ対応デバイスのほとんどにおいて、認証とシグナリング暗号化は、メディアを暗号化するための最小要件です。つまり、デバイスがシグナリング暗号化と認証をサポートしていない場合、メディア暗号化は行われません。CiscoIOS ゲートウェイとトランクは、認証なしでメディア暗号化をサポートします。CiscoIOS ゲートウェイおよびトランクの場合は、SRTP 機能 (メディア暗号化) を有効にするときに 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の SRTP またはシグナリング暗号化を設定する前に、Cisco では、Cisco IOS の転送 CP ゲートウェイ、h.323 ゲートウェイ、および h.323/トランクを使用して ipsec を設定することを強く推奨します。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ために、IPsec 設定に依存します。Unified Communications Manager は、IPsec 接続が正しく設定されていることを確認しません。IPsec を正しく設定しないと、セキュリティ関連の情報が公開される可能性があります。

SIP トランクは TLS に依存して、セキュリティ関連の情報がクリアテキストで送信されないようにします。

次の例では、SCCP コールと転送 CP コールのメディア暗号化を示します。

1. デバイス A とデバイス B は、メディアの暗号化と認証をサポートしており、Unified Communications Manager に登録されています。
2. デバイス A がデバイス B に対してコールを発信すると、Unified Communications Manager はキーマネージャ機能に対しメディアセッションマスター値のセットを2つ要求します。
3. 両方のデバイスが2つのセットを受信します。1セットはメディアストリーム用、デバイス A はデバイス B、メディアストリームの場合はデバイス B (デバイス A) です。
4. デバイス A はマスター値の最初のセットを使用して、メディアストリーム (デバイス A) を暗号化および認証するキーを導出します。
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) を認証および復号化するキーを導出します。
6. デバイス B は、逆の動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すると、デバイスは必要なキー導出を実行し、SRTP パケット処理が行われます。



- (注) SIP を実行している電話と H.323 トランクまたはゲートウェイは、独自の暗号パラメータを生成し、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、会議リソースの保護に関連するトピックを参照してください。

Secure Hash Algorithm (SHA-2) の SCCP ゲートウェイおよびハードウェア会議ブリッジ

Skinny Client Control Protocol (SCCP) では、Unified Communications Manager で Transport Layer Security (TLS) および Secured Real-Time Transport Protocol (SRTP) を使用するシグナリング完全性およびメディアの暗号化によって、Foreign Exchange Station (FXS) アナログエンドポイントが拡張されます。

Unified Communications Manager では、SCCP ゲートウェイ (アナログエンドポイント) およびハードウェア会議ブリッジ (TLS および SRTP) での SHA-2 アルゴリズムのサポートが強化されました。

前提条件

SCCP アナログ エンドポイントおよびハードウェア会議ブリッジの SHA-2 サポートは、次のバージョンおよびゲートウェイ バージョンで機能します。Unified Communications Manager

- Unified CM バージョン 14 SU1 以降。

- ゲートウェイ IOS バージョン：IOS XE 17.6.1 であり、セキュアなシグナリングのために TLS V1.2 をサポートするように設定する必要があります。

**Note**

- アナログエンドポイントの場合、音声ゲートウェイで STCAPP を有効にし、FXS ポートが音声ゲートウェイで使用可能になっていることを確認して、Unified Communications Manager でセキュアな FXS ポートを登録します。
- ハードウェア会議ブリッジの場合、トランスコーディングセッション、MTPセッション、および会議の組み合わせを同時にサポートするため、会議用の安全な DSPFARM プロファイルが必要です。

オーバーライド機能

Unified Communications Manager は、リソースの可用性に応じて、これらの要求を許可または拒否する、ゲートウェイからの会議またはトランスコーディングサービスを要求します。

Cisco Unified OS の管理のユーザーインターフェイスの [暗号管理 (Cipher Management)] ページで暗号を設定していない場合は、**Enterprise Parameters > TLS Ciphers** のデフォルト設定が認識され、ネゴシエートされます。SCCP Cisco IP Phone との下位互換性を避けるために、SCCP FXS はデフォルトで SHA-1 TLS 暗号になっています。

Cisco Unified CM 管理の >[システム (Systems)] > [企業パラメータ (Enterprise Parameter)] > [TLS 暗号 (TLS Ciphers)] フィールドでデフォルトオプションの [すべてのサポートされている暗号 (All Supported Ciphers)] を選択した場合、次の暗号が TLS 接続のために Unified CM によって認識され、ネゴシエートされます。AEAD_AES_256_GCM、AEAD_AES_128_GCM、AES_CM_128_HMAC_SHA1_32、SHA1_80、F8_128_HMAC_SHA1_32、F8_SHA1_80。ただし、**[Cisco Unified OS の管理 (Cisco Unified OS Administration)] > [セキュリティ (Security)] > [暗号管理 (Cipher Management)]** がすべての TLS インターフェイスで

「AES256-GCM-SHA384:AES256-SHA256」に設定されている場合、すべての 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、企業パラメータ値を無視します。詳細については、「暗号文字列の構成」および「暗号の制限」セクションを参照してください。

次に例を示します。

1. **[Cisco Unified OS の管理 (Cisco Unified OS Administration)] >** では [暗号管理 (Cipher Management)] が [デフォルト (Default)] に設定されており、SHA-1 TLS がネゴシエートされます。
2. **Cisco Unified OS の管理 >** では、[暗号管理 (Cipher Management)] が [すべて (ALL)] に設定されており、SHA-2 TLS がネゴシエートされます。

セキュアコールのアルゴリズム

Unified Communications Manager は、セキュアコールで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拡張されています。この機能強化の一環として、SCCP バージョンは Unified Communications Manager でバージョン 23 に引き上げられました。

新しい Open Receive Channel (ORC) および Start Media Transmission (SMT) バージョン 23 構造は、新しい SHA-2 暗号スイートのキーおよびソルトサイズをサポートするために MAX_KEY_SIZE = 32 で実装されます。



Note SHA-2 は、SCCP 電話、H323、および MGCP ではサポートされていません。

SCCP 経路で登録されたアナログエンドポイントのメディアを保護するには、次の手順を実行します。

- Unified CM に登録されている 2 つの安全な SCCP アナログエンドポイント間のコールは、SHA-2 暗号のいずれか (AEAD_AES_256_GCM または AEAD_AES_128_GCM) とネゴシエートする必要があります。
- セキュアな SCCP アナログエンドポイントと、Unified CM に登録されている SHA-2 サポートを持つ SIP エンドポイント間のコールは、SHA-2 暗号のいずれか (AEAD_AES_256_GCM または AEAD_AES_128_GCM) とネゴシエートします。

会議がハードウェア会議ブリッジでホストされているときにメディアを保護するには:

- SHA-2 をサポートする SCCP アナログ エンドポイントまたは SIP エンドポイントが SCCP ハードウェア会議ブリッジに接続されている場合、SHA-2 暗号は AEAD_AES_256_GCM または AEAD_AES_128_GCM をネゴシエートします。
- セキュアな電話会議中に、セキュアな SCCP 会議のエンドポイントにメディア確立アルゴリズムが混在している場合、会議ブリッジはその特定のコールレグで対応するアルゴリズムをネゴシエートします。

TLS および SIP SRTP に対する AES 256 暗号化のサポート

Cisco Collaboration ソリューションは、Transport Layer Security (TLS) および Secure Real-time Transport Protocol (SRTP) を使用し、シグナリングとメディア暗号化を行います。現在、128 ビット暗号キーを使用した Advanced Encryption Standard (AES) は、暗号化暗号として使用されています。AES では、認証方式として Hash-based Message Authentication Code Secure Hash Algorithm-1 (HMAC-SHA-1) も使用されます。これらのアルゴリズムは、必要な変化するセキュリティとパフォーマンスのニーズに合わせて効果的に拡張することはできません。セキュリティとパフォーマンスの要件の増大に対応するため、Next-Generation Encryption (NGE) での、暗号化、認証、デジタル署名、およびキー交換用のアルゴリズムとプロトコルが開発されています。また、TLS および NGE をサポートするセッション開始プロトコル (SIP) SRTP の AES 128 の代わりに、AES 256 暗号化サポートが提供されます。

AES 256 Encryption Support for TLS and SIP SRTP が、シグナリング暗号化とメディア暗号化での AES 256 暗号化のサポートに重点を置くために拡張されています。この機能は、Unified Communications Manager 上で実行されているアプリケーションが、SHA-2 (Secure Hash Algorithm) 標準規格および Federal Information Processing Standards (FIPS) に準拠する、AES-256 ベースの暗号を使用して TLS 1.2 接続を開始してサポートするために役立ちます。

この機能には、次の要件があります。

- SIP トランクと SIP 回線が開始する接続。
- Unified Communications Manager が SIP 回線と SIP トランクを通じた SRTP コール用にサポートする暗号化であること。



(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サポートされているわけではありません。TLS 1.0 および 1.1 は、コラボレーション展開で有効にしたまま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) プロトコルでは、2つのアプリケーション間の通信の認証、データの整合性、および機密性が提供されます。TLS 1.2 はセキュア ソケット レイヤ (SSL) プロトコルバージョン 3.0 をベースにしていますが、これら 2つのプロトコルに相互の互換性はありません。TLS はクライアント/サーバモードで動作し、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します。SSL は、伝送制御プロトコル (TCP) レイヤとアプリケーションの間のプロトコル層として配置され、クライアントとサーバ間のセキュアな接続を形成し、ネットワークを介して安全に通信できるようにします。TLS を動作させるには、信頼性の高い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 における、TLS 1.2 での AES 256 および SHA-2 (Secure Hash Algorithm-2) のサポートは、SIP トランクおよび 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。AES 256 および SHA-2 に準拠する、サポートされる暗号方式は次のとおりです。

- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256: 暗号ストリングは ECDH-RSA-AES128-GCM-SHA256 です。
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384: 暗号ストリングは ECDH-RSA-AES256-GCM-SHA384 です。

定義:

- TLS は、Transport Layer Security です
- ECDH は楕円曲線 Diffie-hellman (アルゴリズム) です。
- RSA is Rivest Shamir Adleman (アルゴリズム)
- AES は、Advanced Encryption Standards です

- GCM は、Galois/Counter Mode です

新しくサポートされた暗号方式に加えて、Unified Communications Manager では、TLS_RSA_WITH_AES_128_CBC_SHA が引き続きサポートされています。この暗号方式の暗号ストリングは AES128-SHA です。



- (注)
- Unified Communications Manager の証明書は、RSA に基づいています。
 - Unified Communications Manager では、シスコの各エンドポイント（各電話）で、上記の TLS 1.2 用の新しい暗号方式はサポートされません。
 - Unified Communications Manager において TLS 1.2 での AES 256 および SHA-2（Secure Hash Algorithm-2）のサポート機能強化を使用すると、Certificate Authority Proxy Function（CAPF）のデフォルトのキー サイズが 2048 ビットに増えます。

SRTP SIP コールシグナリングでの AES 256 のサポート

Secure Real time Transport Protocol (SRTP) は、リアルタイムトランスポートプロトコル (RTP) の音声およびビデオメディアと、それに対応するリアルタイムトランスポート制御プロトコル (RTCP) ストリームの両方に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、暗号化およびメッセージ認証ヘッダーを使用してこの方式を実装します。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 のヘッダーと RTP のペイロードの両方に適用されます。また、メッセージ認証がヘッダー内の RTP のシーケンス番号に適用されるため、SRTP ではリプレイアタックに対する保護も間接的に提供されます。SRTP は、暗号化方法として 128 ビットの暗号キーによる Advanced Encryption Standard (AES) を使用します。また、認証方式として、Hash-based Message Authentication Code Secure Hash Algorithm-1 (HMAC-SHA-1) も使用します。

Unified Communications Manager では、SIP 回線と SIP トランクを通じた SRTP コール用の暗号方式がサポートされます。これらの暗号暗号方式は AEAD_AES_256_GCM と AEAD_AES_128_GCM であり、AEAD は関連データを使用して認証され、GCM は Galois/Counter モードです。これらの暗号方式は GCM に基づいています。これらの暗号方式が Session Description Protocol (SDP) に存在する場合、AES 128 および SHA-1 ベースの暗号方式よりも高いプライオリティで処理されます。シスコの各エンドポイント（電話）では、Unified Communications Manager に SRTP のために追加した、これらの新しい暗号方式はサポートされません。

新たにサポートされる暗号方式に加えて、Unified Communications Manager では次の暗号方式が引き続きサポートされます。

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- F8_128_HMAC_SHA1_80

AES 256 暗号化は、次のコール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 のサポートを使用できます。
- 暗号サポート: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (暗号ストリング ECDHE-AES256 SHA384) および TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (暗号ストリング ECDHE-AES128): TLS 1.2 接続が確立されたときに使用可能になります。これらの暗号方式は 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 暗号方式と TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 暗号方式を使用して TLS 1.2 を開始します。ピアが TLS 1.2 をサポートしていない場合、Unified Communications Manager は既存の AES128-SHA 暗号方式を使用した TLS 1.0 にフォールバックします。
- SIP 回線および SIP トランクを介した SRTP コールは、GCM ベースの AEAD_AES_256_GCM と AEAD_AES_128_GCM の暗号方式をサポートします。

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 間コールのみに適用されます。
- 非 SIP 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。Skinny Call Control Protocol (SCCP) は、以前にサポートされていた暗号方式を使用した TLS 1.2 もサポートしています。
- Sip から非 SIP へのコールでは、引き続き AES 128 および SHA-1 ベースの暗号方式が使用されます。

AES 80 ビット認証サポート

Unified Communications Manager は、128 ビット暗号化キーと 80 ビット認証タグを保留音 (MOH)、自動音声応答 (IVR)、アナウンサーの暗号化アルゴリズムとして使用する Advanced Encryption Standard (AES) をサポートしています。デフォルトでは、80 ビット認証タグをサポートする電話機は、AES_CM_128_HMAC_SHA1_80 crypto 暗号方式を使用して MOH、IVR、および警報を再生します。

電話機が IP Voice Media Streaming (IPVMS) に安全に接続すると、AES_CM_128_HMAC_SHA1_80 crypto cipher に優先順位が付与されます。電話機が 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 ビットの認証タグのいずれかをサポートしていない場合は、Real-time Transport Protocol (RTP) でネゴシエーションを行います。



- (注) SCCC 電話は 32 ビット認証タグしかサポートしていません。そのため、電話と IPVMS とのネゴシエーションは、AES_CM_128_HMAC_SHA1_32 暗号でのみ行われます。

電話 A が AES_CM_128_HMAC_SHA1_80 暗号化アルゴリズムをサポートし、電話 B が AES_CM_128_HMAC_SHA1_32 暗号化アルゴリズムをサポートしている場合、ユーザ A（電話 A）がユーザ B（電話 B）にダイヤルしユーザ B が保留にすると、ユーザ A は MOH に接続されます。電話 A は 80 ビット認証タグしかサポートしないため、電話 A と MOH のネゴシエーションは AES_CM_128_HMAC_SHA1_80 暗号を介して行われます。

ユーザ B（電話 B）がユーザ A（電話 A）にダイヤルし、ユーザ A が保留にすると、電話 B は 32 ビット認証タグしかサポートしていないので、電話 B と MOH のネゴシエーションは AES_CM_128_HMAC_SHA1_32 暗号により行われます。

電話が 80 ビット認証タグをサポートする場合、電話と IVR またはアナウンサーとのネゴシエーションは AES_CM_128_HMAC_SHA1_80 で行われます。

次の表は、電話がサポートする暗号化アルゴリズムとネゴシエーション暗号を示しています。

表 5: 電話機能とネゴシエートされた暗号方式の比較

| 電話がサポートする暗号化アルゴリズム | ネゴシエートされた暗号 |
|--|-------------------------|
| AES_CM_128_HMAC_SHA1_32 と 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 と AES_CM_128_HMAC_SHA1_80 以外 | RTP に戻ります。 |

メディアストリーミングデバイスとの SRTP 暗号の不一致

セキュアコールが保留、IVR、またはアナウンサーアナウンスなどの機能呼び出ししているときに、リモートの発信者が打診転送を実行すると、新しいコールレグは MOH、IVR、またはアナウンサーとは異なる暗号機能をサポートする場合があります。これにより、暗号の不一致が発生し、エンドポイントの SRTP フォールバックオプションに応じて、コールは非セキュアモードにドロップされるか、完全にドロップされます。**Unified Communications Manager** の [システム (System)] > [サービス パラメータ (Service Parameters)] > [サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウで [暗号化されていないコールをブロック (Block Unencrypted Calls)] サービスパラメータが [True] に設定されている場合でも、セキュアコールはドロップされます。

Unified Communications Manager プラットフォームの新しい拡張機能により、Cisco IP Voice Media Streaming (IPVMS) デバイス (MOH、IVR、またはアナウンサー) 以降のコール機能を交換

するときに、すべての暗号方式がサポートされます。SRTP フォールバック構成はアクティブコールに影響を与えず、セキュリティも損なわれません。



Note メディア デバイスは、SHA1_32 および SHA1_80 ビットの暗号化方式のみをサポートします。

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、ハードドライブで使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式です。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。ディスク上の使用可能なハードウェアは、すべての受信データを暗号化し、すべての送信データの暗号化を解除します。

ドライブがロックされると、暗号化キーが内部で作成され保存されます。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 キーで構成されます。

詳細については、『[Cisco UCS C シリーズサーバー Integrated Management Controller GUI コンフィギュレーションガイド](#)』を参照してください。

設定ファイルの暗号化

Unified Communications Manager は、ダイジェスト クレデンシャルや管理者パスワードといった機密データを、TFTP サーバからの設定ファイルダウンロードの形で電話にプッシュします。

Unified Communications Manager において、データベース内では可逆暗号化を使用してこれらのクレデンシャルが保護されています。ダウンロードプロセス中のデータを保護するため、このオプションをサポートするすべての Cisco IP 電話において、暗号化された設定ファイルを設定することを推奨します。このオプションを有効にすると、デバイスコンフィギュレーションファイルだけがダウンロード用に暗号化されます。



(注) 状況によっては、暗号化されていない電話機に機密データを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、電話機のトラブルシューティングなどです。

Unified Communications Manager は、暗号化キーを符号化してデータベースに保存します。TFTP サーバでは、対称暗号化キーを使用して設定ファイルの暗号化と復号が行われます。

- 電話に PKI 機能がある場合、Unified Communications Manager では電話の公開キーを使用して電話の設定ファイルを暗号化できます。
- 電話に PKI 機能がない場合、Unified Communications Manager と電話に一意の対称キーを設定する必要があります。

暗号化設定ファイルの設定は、[Unified Communications Manager Administration] の [Phone Security Profile] ウィンドウで有効化し、その後 [Phone Configuration] ウィンドウで電話に適用します。

デフォルトのセキュリティ管理タスク

デフォルトのセキュリティ管理タスクを以下に示します。

手順

| | コマンドまたはアクション | 目的 |
|--------|-----------------------------------|---|
| ステップ 1 | Cisco Unified IP 電話 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 | ITL ファイルステータスの取得 | 電話機の ITL ファイルステータスを取得します。 |
| ステップ 3 | Cisco Unified IP 電話 サポートリストの取得 | Cisco Unified Reporting ページを使用して Cisco Unified IP Phone のサポートリストを取得します。 |
| ステップ 4 | 8.0 より前のリリースへのクラスタのロールバック | ロールバック用のクラスタを準備します。 |
| ステップ 5 | ITL ファイルの一括リセットの実行 (41 ページ) | ITL ファイルの一括リセットの実行 |
| ステップ 6 | CTL ローカルキーのリセット | CLI コマンドを使用して Cisco Trust List (CTL) ファイルのリセットを実行する |
| ステップ 7 | ITLRecovery 証明書の有効期間の表示 | ITLRecovery 証明書の有効期間を表示します。 |
| ステップ 8 | 認証と暗号化のセットアップ | 新規インストールの認証と暗号化を実装します。 |

Cisco Unified IP 電話 の ITL ファイルの更新

電話機にインストールされている ITL ファイルでデフォルトのセキュリティを使用している Unified Communication Manager との集中型 TFTP では、TFTP 設定ファイルは検証されません。

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

- ステップ 1 中央 TFTP サーバで、Enterprise パラメータ **Prepare cluster for PRE CM-8.0 rollback** 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 すべての電話機をリセットして、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ていることを確認します。
- ステップ 4 HTTPS ではなく 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 のリリース 10.5 以降では、[クラスタの 8.0 以前へのロールバック準備 (Prepare Cluster for Rollback to pre-8.0)] エンタープライズ パラメータを有効にした後、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 バージョンと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 より前のリリースへのクラスタのロールバック」セクションを参照してください。

ITL ファイルステータスの取得

電話機の ITL ファイルステータスを取得するには、次の手順を使用します。

- ステップ 1 Cisco Unified Communications Manager Administration から、[デバイス (Device)] > [電話 (Phone)] を選択します。
- ステップ 2 [電話機を探す (Find Phone where)] ドロップダウンリストで [ITL ファイルステータス (ITL File Status)] を選択し、条件を選択します。

| フィールド | 説明 |
|---------------|--|
| Match | サーバーと電話機の ITL ハッシュが同じ |
| MisMatch | サーバーの ITL ハッシュが電話の ITL ハッシュではない、または電話またはサーバーの ITL ハッシュが不明です。 |
| Not Installed | 電話機が新しい CUCM サーバーへの登録に失敗し、以前のサーバーにバウンズする |

- ステップ 3 [検索 (Find)] をクリックします。

Cisco Unified IP 電話 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シスコエンドポイントのリストを生成します。

- 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 [システムレポート (System Reports)] リストで、[Unified CM 電話機能一覧 (Unified CM Phone Feature List)] をクリックします。
- ステップ 3 [製品 (Product)] ドロップダウンリストから、[デフォルトのセキュリティ (Security By Default)] 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。

8.0 より前のリリースへのクラスタのロールバック

クラスタを Unified Communications Manager の旧リリース（リリース 8.0 よりも前）にロールバックする場合は、その前に [Prepare Cluster for Rollback to pre-8.0] エンタープライズパラメータを使用したロールバックの準備が必要です。

クラスタをロールバックするための準備を行うには、クラスタの各サーバで次の手順に従います。

ステップ 1 Unified Communications Manager で、[システム (System)] > [エンタープライズパラメータ設定 (Enterprise Parameters Configuration)] を選択します。

[Enterprise Parameters Configuration] ウィンドウが表示されます。

[Prepare Cluster for Rollback to pre-8.0] エンタープライズパラメータを [True] に設定します。

(注) クラスタを Unified Communications Manager のバージョン 8.0 以前へロールバックする準備を行う場合のみ、このパラメータを有効にします。このパラメータが有効になっている間、HTTPS を使う電話サービス（たとえば、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ても、基本的な電話の発信および受信は引き続き可能です。

ステップ 2 Cisco IP 電話が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

ステップ 3 クラスタの各サーバを以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 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 4 クラスタが以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 次のリリースのいずれかを混合モードで実行している場合、CTL クライアントの実行が必要です。

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

(注) CTL クライアントの実行方法の詳細については、「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 「Prepare Cluster for Rollback to pre-8.0」 エンタープライズパラメータが [True] に設定されている場合、社内ディレクトリが機能するために以下の変更が必要です。

[Device] > [Device Settings] > [Phone Services] > [Corporate Directory] で、サービス URL を「Application: Cisco/CorporateDirectory」から「http://<ipaddr>:8080/ccmcip/xmldirectoryinput.jsp」へと変更します。

ステップ 7 「[Prepare Cluster for Rollback to pre-8.0]」 エンタープライズ パラメータが [True] に設定されている場合、パーソナルディレクトリが機能するために以下の変更が必要です。

[Device] > [Device Settings] > [Phone Services] > [Personal Directory] で、サービス URL を「Application: Cisco/PersonalDirectory」から「http://<ipaddr>:8080/ccmpd/pdCheckLogin.do?name=undefined」へと変更します。

復帰後のリリース8.6以降へのスイッチバック

クラスタをリリース7.xに戻した後にリリース8.6またはそれ以降のパーティションに切り替える場合は、次の手順に従います。

ステップ 1 クラスタを非アクティブのパーティションに再度切り替えるための手順に従います。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 次のいずれかのリリースを混合モードで使用していた場合は、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
- 007.001 (002.32016.001) より前の712のすべての ES リリース
- Unified Communications Manager リリース 7.1(3)

- 007.001 (003.21900.003) より前の713のすべての通常リリース = 7.1 (3a) sula

- 007.001 (003.21005.001) より前の713のすべての ES リリース

(注) CTL クライアントの実行方法の詳細については、「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、[System] > [Enterprise Parameters Configuration] を選択します。

[Enterprise Parameters Configuration] ウィンドウが表示されます。

[Prepare Cluster for Rollback to pre-8.6] エンタープライズ パラメータを [False] に設定します。

ステップ 4 Cisco Unified IP 電話 が自動的に再起動され、Unified Communications Manager に登録されるまで、10 分間待ちます。

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 パブリッシャで実行してください。

電話機が ITL ファイル 署名者を信頼できなくなり、かつ TFTP サービスによってローカルに提供された ITL ファイルを認証できないか、TVS を使用して認証できない場合は、ITL ファイルの一括リセットが実行されます。

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 リカバリファイルを生成し、電話機と CUCM の TFTP サービス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は、CLI コマンド **file get tftp ITLRecovery.p12** を使用して ITL リカバリペアをエクスポートしてから、DR を介してバックアップを実行します。（キーのエクスポート先となる）SFTP サーバとパスワードの入力を求めるプロンプトも表示されます。

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にあります。このコマンドを発行しているとき、ITL 回復キーをリセットしている間、ITL ファイルは 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正常に行われたことを確認します。

ステップ 3 Cisco Unified CM Administration から、[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。

ステップ 4 [Reset] をクリックします。

デバイスが再起動されます。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、設定ファイルを受け入れる準備が整いました。

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 キーによって署名され、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、再度ユニファイドコミュニケーションマネージャに登録します。

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、信頼されたステータスが失われる場合は、CLI コマンド **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。

ステップ 1 **utils ctl reset localkey** の実行

(注) **utils ctl reset localkey** では、ローカルキーはパブリッシャ側にあります。このコマンドを発行すると、CTL ファイルは ITLRecovery キーによって一時的に署名されます。

ステップ 2 リセットが正常に行われたことを確認するには **show ctl** を実行します。

ステップ 3 Cisco Unified CM Administration から、[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の設定 (Enterprise Parameters Configuration)] ページが表示されます。

ステップ 4 [Reset] をクリックします。

デバイスが再起動されます。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、設定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** を実行して、ステップ 1 の変更をロールバックする必要なサービスを再起動します。

デバイスが再起動されます。これで、ITLRecovery キーで署名された CTL ファイルをダウンロードし、設定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、Unified Communications Manager に再度正しく登録します。

ITLRecovery 証明書の有効期間の表示

ITLRecovery 証明書は電話機での有効期間が長いです。[証明書ファイルデータ (Certificate File Data)] ペインに移動し、有効期間または他の ITLRecovery 証明書の詳細を表示できます。

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 証明書を検索し、設定の詳細を表示するには、必要な検索パラメータを入力します。
条件に一致する証明書のリストが [証明書リスト (Certificate List)] ページに表示されます。

ステップ 3 [ITLRecovery] リンクをクリックして、有効期間を確認します。

ITLRecovery 証明書の詳細が [証明書ファイルデータ (Certificate File Data)] ペインに表示されます。

有効期間は現在の年から 20 年です。

認証と暗号化のセットアップ



重要 `utilsctl` CLI コマンドセットを使用して、暗号化を設定することができます。このオプションの詳細については、『*Command Line Interface Guide for Cisco Unified Communications Solutions*』を参照してください。

次の手順では、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について説明します。指定されたセキュリティ機能に対して実行する必要があるタスクを含む章の参考資料については、「関連項目」を参照してください。

- 新規インストールの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。
- ノードをセキュアクラスタに追加するには、ノードの追加方法および新しいノード用のセキュリティの設定方法を説明している『*Installing Cisco Unified Communications Manager*』を参照してください。



第 II 部

基本的なシステムセキュリティ

- 証明書 (47 ページ)
- Certificate Authority Proxy Function (81 ページ)
- セキュリティモード (101 ページ)
- SIP OAuth モード (107 ページ)
- TFTP 暗号化 (117 ページ)
- 暗号管理 (125 ページ)
- 電話機のセキュリティ (145 ページ)
- セキュアな会議リソースの設定 (183 ページ)
- ボイス メッセージング ポートのセキュリティ設定 (199 ページ)
- セキュアトーンとアイコン (205 ページ)
- トランクとゲートウェイの SIP セキュリティ (215 ページ)
- TLS セットアップ (233 ページ)



第 5 章

証明書

- [証明書の管理](#) (47 ページ)
- [証明書のモニタリングと失効タスクのフロー](#) (74 ページ)
- [簡素化された証明書管理](#) (78 ページ)

証明書の管理

証明書管理機能は、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、および証明書をモニタおよび失効させる方法の概要を提供します。

証明書概要

証明書は、導入でセキュアな接続を確立するために不可欠です。ネットワーク上で個人、コンピュータ、および他のサービスを認証します。適切な証明書管理を実施することで、適切なレベルの保護を実現し、かつ複雑さを軽減できます。

証明書は、証明書所有者のアイデンティティを証明するファイルであり、次の情報が含まれます。

- 証明書所有者の名前
- 公開キー
- 証明書を発行する認証局のデジタル署名

Unified Communications Manager は、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するために、Public Key Infrastructure (PKI) を使用する証明書を使用します。適切な信頼ストアに一致する証明書がある場合を除き、他のシステムは信頼されず、アクセスが拒否されます。

ルート証明書は、デバイスやアプリケーションユーザなど、ユーザとホスト間のセキュアな接続を確保します。証明書は、クライアントとサーバのアイデンティティの安全性を確保し、これらをルート信頼ストアに追加します。

管理者は、サーバ証明書のフィンガープリントを表示し、自己署名証明書を再生成して、Unified Communications Manager インターフェイスから信頼証明書を削除できます。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 信頼ストアを更新して証明書を管理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』を参照してください。



(注) Unified Communications Manager は、PEM (.pem) 形式および DER (.der) 形式の証明書のみサポートします。DER あるいは PEM の証明書のサポートされる最大サイズは 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。例：*.cisco.com



(注) いずれかの Unified Communications Manager 信頼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は、これらの名前と有効期間は同じであるが、シリアル番号と署名アルゴリズムが異なっていることを確認してください。

例：

27:20:41:0c:5b:08:69:80:42:62:4f:13:bd:16:06:6a シリアル番号と SHA-1 アルゴリズムを持つルート CA が 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 シリアル番号と 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、証明書管理は次の処理を実行します。

- 着信証明書の有効性を確認します。
- tomcatTomcat 信頼フォルダ内にある同じ名前前の証明書を検索します
- Tomcat 信頼フォルダにある既存の証明書のシリアル番号と、アップロードされている着信証明書のシリアル番号を比較します。

それらのシリアル番号が異なる場合は、両方の証明書の有効期限開始日を確認します。新しい着信証明書の開始タイムスタンプが最新の場合は、既存の証明書は置き換えられ、そうでない場合はアップロードされません。

SHA-1 と SHA-256 のアルゴリズムでは、件名または共通名が同じであれば、同じエンティティに属していることを意味しています。この Unified Communications Manager フレームワークは、Unified Communications Manager サーバ上でこれら両方のアルゴリズムを同時にサポートしませ

ん。特定の信頼フォルダ内では、署名アルゴリズムが何であれ、いずれかのエンティティに属する 1 つの証明書のみがサポートされます。

証明書タイプ

このセクションでは、さまざまな種類の証明書と証明書署名要求、キーの用途拡張の概要を説明します。

電話機の証明書タイプ

電話機証明書は、電話機を認証するための一意の識別子です。これは、IP 攻撃に対するセキュリティにとって重要です。

電話機の証明書は次のとおりです。

表 6:

| 電話機の証明書 | 説明 |
|------------------------|---|
| 製造元でインストールされる証明書 (MIC) | MIC は Cisco Manufacturing CA によって署名され、署名された証明書はサポートされている Cisco Unified IP Phone に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) のインストールまたは暗号化された設定ファイルのダウンロードに対して、シスコ認証局プロキシ機能 (CAPF) で認証します。管理者は証明書を変更、削除、または無効にできないため、有効期限が切れた後は使用できません。 |
| ローカルで有効な証明書 (LSC) | Cisco Unified IP Phone は、セキュアモードで動作するために LSC を必要とし、認証と暗号化に使用されます。これらは CAPF、オンラインまたはオフライン CA により署名され、MIC よりも優先されます。 CAPF に関連付けられている必要なタスクを実行すると、サポートされている電話機にこの証明書がインストールされます。認証または暗号化を使用するようにデバイスセキュリティモードを設定した後に、LSC により、Unified Communications Manager と電話機間の接続のセキュリティが確保されます。 |



ヒント MIC は LSC のインストール時にのみ使用することを推奨します。シスコでは、Unified Communications Manager との TLS 接続の認証用に LSC をサポートしています。電話の設定で TLS 認証などの目的で MIC を使用した場合、MIC ルート証明書は容易に侵害されるため、当社は何ら責任を負いません

Unified Communications Manager への TLS 接続に LSC を使用するには、Cisco Unified IP Phone 6900、7900、8900、および 9900 シリーズをアップグレードします。今後の互換性の問題を回

避するために、Unified Communications Manager 信頼ストアから MIC ルート証明書を削除します。



(注) Unified Communications Manager への TLS 接続に MIC を使用する一部の電話機モデルは、登録できない場合があります。

管理者は Unified Communications Manager 信頼ストアから次の MIC ルート証明書を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 信頼ストアに残された 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) CAP-RTP-001 および CAP-RTP-002 証明書は、Unified Communications Manager から削除されます。



(注) Unified Communications Manager リリース 12.5.1SU2 以前では、Cisco Manufacturing 証明書を CallManger 信頼ストアから削除すると、電話機の製造元でインストールされた証明書 (MIC) を検証できないため、セキュアオンボーディング機能は動作しません。ただし、Unified Communications Manager リリース 12.5.1SU3 以降では、CAPF 信頼ストアを使用して電話機の MIC を検証するため、この機能は動作します。

サーバ証明書のタイプ

サーバ証明書は、基本的にサーバを識別するための証明書です。サーバ証明書は、コンテンツを暗号化および復号化する論拠の役目を果たします。

Unified Communications Manager サーバ内の自己署名証明書 (所有) 証明書タイプは次のとおりです。

Unified Communications Manager は次の証明書タイプを Unified Communications Manager 信頼ストアにインポートします。

表 7: 証明書タイプと説明

| 証明書タイプ | 説明 |
|---|---|
| Cisco Unity サーバまたは Cisco Unity Connection 証明書 | Cisco Unity と Cisco Unity Connection は、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 デバイス証明書に署名します。Cisco unity の場合、Cisco Unity TELEPHONY Integration Manager (UTIM) はこの証明書を管理します。Cisco Unity Connection の場合は、Cisco Unity Connection の管理機能がこの証明書を管理します。 |
| 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 | 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、SIP ユーザー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、SIP トランク経由で接続する SIP ユーザーエージェントは、Unified Communications Manager に対して認証されます。 |



(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) は、ルート証明書をルートとする証明書を発行します。

次の追加の信頼ストアが存在します。

- tomcat および web アプリケーションの共通信頼ストア
- IPSec-trust
- CAPF-trust
- Userlicensing: 信頼
- TVS-trust
- Phone-SAST-trust
- Phone-CTL-trust

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、電子メール、予定表情報、連絡先を取得するための Exchange または Meeting Place Express へのセキュアな接続を確保します。

サードパーティー CA 署名付き証明書

CA で署名された証明書は、デジタル証明書に署名および発行する信頼できるサードパーティー証明書です。

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。ただし、証明書に署名するようにサードパーティー CA を設定することによって、セキュリティを追加できます。サードパーティー CA を使用するには、CA ルート証明書チェーンを Cisco Unified Communications Manager Administration にインストールします。

CA で署名された証明書を発行するには、CA が証明書を発行して署名できるように証明書署名要求 (CSR) を提出する必要があります。証明書をアップロード、ダウンロード、および表示する方法の詳細については、「自己署名証明書」セクションを参照してください。

構成

Unified Communications Manager に接続している別のシステムからの CA で署名された証明書を使用する場合は、Cisco Unified Communications Manager Administration で次の手順を実行します。

- 証明書を署名した CA のルート証明書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。

CA で署名された証明書を Unified Communications Manager で使用する場合は、次の手順に従います。

- Cisco Unified Communications Manager Administration で CA で署名された証明書を要求するには、CSR を完了します。
- CA ルート証明書チェーンと CA で署名された証明書の両方を次のページでダウンロードします。Cisco Unified Communications Manager Administration
- CA ルート証明書チェーンと CA で署名された証明書の両方をアップロードします。

CA のルート証明書の取得と設定の方法の詳細については、証明機関のマニュアル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、PKCS#10 Certificate Signing Request (CSR; 証明書署名要求) メカニズムを使用して、サードパーティーの認証局 (CA) との統合をサポートします。このメカニズムには、Unified Communications Manager の GUI でアクセスできます。

現在、サードパーティー CA を使用しているお客様は、CSR メカニズムを使用して次の証明書を発行する必要があります。

- Unified Communications Manager
- CAPF
- IPSec

- Tomcat
- 信頼検証サービス (TVS)



(注) マルチサーバ (SAN) の CA 署名付き証明書は、証明書が発行元にアップロードされた場合にのみクラスタ内のノードに適用されます。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したり、再作成するたびにクラスタにアップロードします。

システムを混合モードで実行すると、一部のエンドポイントでは、キーサイズが4096以上の CA 証明書を受け入れることができない場合があります。混合モードで CA 証明書を使用するには、次のいずれかのオプションを選択します。

- 証明書のキーサイズが 4096 未満の証明書を使用します。
- 自己署名証明書を使用します。



(注) Cisco の CTL クライアントは、リリース 14 からサポートされなくなりました。Cisco CTL プラグインではなく、CLI コマンドを使用して、Unified Communications Manager サーバーを混合モードに切り替えることをお勧めします。

CTL クライアントを実行した後、該当するサービスを再起動して更新します。

例：

- Unified Communications Manager 証明書を更新する際に、TFTP サービスと Unified Communications Manager サービスを再起動します。
- CAPF 証明書を更新するときに 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に、ITL ファイルを更新するために自動的に電話がリセットされる場合があります。

プラットフォームでの証明書署名要求 (CSR) の生成方法については、『[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

次の表には、Unified Communications Manager と IM and Presence Service の CA 証明書の証明書署名要求 (CSR) のキーの用途拡張が表示されています。

表 8: Cisco Unified Communications Manager CSR キーの用途拡張

| | マルチサーバ | キーの拡張用途 | | | キーの用途 | | | | |
|----------------------------------|--------|------------------------------|-------------------------------------|---|--------|-------|-------------|-------------|-----|
| | | 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 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 | キー証明書署 名 | 鍵共有 |
| CallManager CallManager-ECDSA | Y | Y | Y | | Y | N | Y | | |
| CAPF (パブリッシャ のみ) | N | Y | N | | Y | N | | Y | |
| ipsec | N | Y | Y | Y | Y | Y | Y | | |
| tomcat tomcat-ECDSA | Y | Y | Y | | Y | N | Y | | |
| 信頼検証サービス (TVS) | N | Y | Y | | Y | Y | Y | | |

表 9: IM and Presence Service CSR キーの用途拡張

| | マルチサーバ | キーの拡張用途 | | | キーの用途 | | | | |
|------------------------------------|--------|------------------------------|-------------------------------------|---|--------|-------|-------------|-------------|-----|
| | | 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 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 | キー証明書署 名 | 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) CA 署名証明書のプロセスの一部として、「データ暗号化」ビットが変更または削除されていないことを確認します。

証明書タスク

このセクションでは、証明書を管理するすべての手順を示します。

証明書の一括エクスポート

新旧のクラスタが同時にオンラインになっている場合には証明書の一括移行による方法を使用できます。

Cisco Unified IP 電話は、ダウンロードしたすべてのファイルを、ITL ファイルまたは ITL ファイルに指定されている TVS サーバと照合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示する ITL ファイルは、古いクラスタの TVS 証明書ストアの信頼を得る必要があります。



(注) 証明書の一括エクスポートは、電話の移行中、両方のクラスタがネットワークに接続され、オンラインである場合のみ機能します。



(注) 証明書一括インポート中、Cisco Extension Mobility Cross Cluster (EMCC) が動作を継続するには、訪問クラスタとホームクラスタの両方において付加的な ITLRecovery 証明書をインポートすることが必要です。[証明書の一括管理 (Bulk Certificate Management)] の [証明書タイプ (Certificate Type)] ドロップダウンリストに、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追加されています。

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。

- ステップ 1 [Cisco Unified Operating System Administration] から、[Security] > [Bulk Certificate Management] を選択します。
- ステップ 2 新しい宛先のクラスタ (TFTP のみ) から中央 SFTP サーバに証明書をエクスポートします。
- ステップ 3 証明書の一括処理用のインターフェイスを使用して SFTP サーバで証明書 (TFTP のみ) を統合します。
- ステップ 4 元のクラスタで証明書の一括機能を使用し、中央 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、またはその他の方法を使用して、電話機に新しい宛先クラスタを指定します。

電話は新しい宛先クラスタの ITL ファイルをダウンロードし、既存の ITL ファイルと照合することを試みます。証明書は既存の ITL ファイル内に存在しないため、電話は古い TVS サーバに新しい ITL ファイルの署名の確認を要求します。電話機は TCP ポート 2445 の古いクラスタに TVS クエリを送信してこの要求を行います。

証明書のエクスポート、統合、インポートが正常に行われると、TVS は成功を返し、電話のメモリにある ITL ファイルは新しくダウンロードされた ITL ファイルに置き換わります。

これで電話機は新しいクラスタから署名付きのコンフィギュレーションファイルをダウンロードし、検証できるようになります。

証明書の表示

証明書の一覧を共通名、有効期限、キータイプ、使用法に基づいて並べ替えて表示するには、[証明書の一覧 (Certificate List)] ページでフィルタオプションを使用します。フィルタオプションにより、データの並べ替え、表示、管理を効率的に行うことができます。

Unified Communications Manager リリース 14 以降では、アイデンティティ証明書または信頼証明書の一覧を並べ替えて表示するときの基準として、使用法オプションを選択できます。

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 [証明書の一覧の検索条件 (Find Certificate List where)] ドロップダウンリストから目的のフィルタオプションを選択し、[検索 (Find)] フィールドに検索項目を入力して、[検索 (Find)] 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。

BCFIPS プロバイダーの証明書表示データは、リリース 14SU2 以降で変更されました。

| 14SU1 までのタグ名 | 14SU2 からのタグ名 |
|--------------|--------------------|
| 発行者名 | 発行者 DN |
| 有効期限 | 開始日 |
| 送信先 | 最終日 |
| サブジェクト名 | サブジェクト DN |
| キー | 公開キー (3Public Key) |
| キー値 | モジュラス |

(注) x509 拡張機能は、実際のキー使用法名ではなく OID 名で表示されます。

証明書のダウンロード

CSR 要求を送信する場合は、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。

ステップ 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。

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 (Download)] 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している場合にのみ必要です。

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 (Upload Certificate/Certificate chain)] をクリックします。

ステップ3 ルート証明書をインストールするには、[証明書の目的 (Certificate Purpose)] ドロップダウンリストから適切な信頼ストアを選択します。

ステップ4 選択した証明書の目的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)
- Tomcat 証明書をアップロードするときは、TFTP サービスを再起動します。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、パブリッシュャ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。

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。
 - 電話エッジトラストからの証明書の削除は、パブリッシャ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。
-

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 (Generate Certificate Signing Request)] 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 [生成 (Generate)] をクリックします。

証明書署名要求のフィールド

表 10: 証明書署名要求のフィールド

| フィールド | 説明 |
|--|--|
| Certificate Purpose | ド롭ダウンリストから、値を選択します。 <ul style="list-style-type: none"> • CallManager • CallManager-ECDSA |
| Distribution | Unified Communications Manager サーバを選択します。 ECDSA の MultiServer にこのフィールドを選択すると、構文は次のとおりです。 Callmanager-ecdsa common name: <host-name>-EC-ms.<domain> RSA の MultiServer にこのフィールドを選択すると、構文は次のとおりです。 Callmanager common name: <host-name>-ms.<domain> |
| Common Name / Common 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 Common Name_SerialNumber は、証明書のファイル名です。 デフォルトでは、 [Distribution] フィールドで選択した Unified Communications Manager アプリケーションの名前が表示されます。 |
| Include OU in CSR | 重要 リリース 14SU1 以降でサポートされます。 デフォルトでは、組織単位フィールドは証明書署名要求から削除されています。証明書署名要求に組織単位フィールドを含めるには、このオプションを選択します。 (注) 証明書署名要求に組織単位があり、署名付き CA 証明書にない場合は、署名付き CA 証明書を Unified Communications Manager にアップロードできます。 |
| Auto-populated Domains | このフィールドは、サブジェクト代替名 (SANs) セクションに表示されます。単一の証明書によって保護されるホスト名が一覧表示されます。 |
| Parent Domain | このフィールドは [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を表示します。必要に応じて、ドメイン名を変更できます。 |

| フィールド | 説明 |
|----------------|--|
| Key Type | <p>このフィールドは、公開キーと秘密キーのペアの暗号化と復号化に使用されるキーのタイプを示します。</p> <p>Unified Communications Manager は EC および RSA キー タイプをサポートしています。</p> |
| Key Length | <p>[キー長 (Key Length)] ドロップダウンリストから、値の1つを選択します。</p> <p>キーの長さによっては、CSR 要求によって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を限定して選択することで、キー長の強度以上のハッシュアルゴリズム強度を使用できます。たとえば、キーの長さが256の場合、サポートされているハッシュアルゴリズムは SHA256、SHA384、またはSHA512です。同様に、384のキー長の場合、サポートされているハッシュアルゴリズムは SHA384 または SHA512 です。</p> <p>(注) キー長の値が3072または4096の証明書は、RSA 証明書に対してのみ選択できます。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。</p> <p>(注) 一部の電話機モデルでは、CallManager の [証明書の目的 (Certificate Purpose)] に対して選択された RSA の [キーの長さ (key length)] が 2048 を超える場合、登録に失敗します。Cisco Unified Reporting Tool (CURT) の [Unified CM Phone Feature List Report] で、3072/4096 RSA キー サイズ サポート機能をサポートする電話モデルの一覧を確認できます。</p> |
| Hash Algorithm | <p>[ハッシュアルゴリズム (Hash Algorithm)] ドロップダウンリストから値を選択して、楕円曲線のキー長としてより強力なハッシュアルゴリズムを設定します。[ハッシュアルゴリズム (Hash Algorithm)] ドロップダウンリストから、値の1つを選択します。</p> <p>(注)</p> <ul style="list-style-type: none"> • [ハッシュアルゴリズム (Hash Algorithm)] フィールドの値は、[キー長 (Key Length)] フィールドで選択した値に基づいて変わります。 • システムが FIPS モードで実行されている場合は、必ずハッシュアルゴリズムとして SHA256 を選択する必要があります。 |

証明書署名要求のダウンロード

CSR を生成した後にダウンロードし、認証局に提出する準備をします。

-
- ステップ 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。
 - 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

-
- ステップ 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。
[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** 新しい自己署名証明書を生成するには、[Generate Self-Signed Certificate] をクリックします。
[Generate New Self-Signed Certificate] ウィンドウが表示されます。
 - ステップ 4** [Certificate Purpose] ドロップダウンボックスから、[CallManager-ECDSA] などのシステムセキュリティ証明書を選択します。
 - ステップ 5** [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** [生成 (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](#) (62 ページ)

自己署名証明書のフィールド

表 11: 自己署名証明書のフィールド

| フィールド | 説明 |
|--|--|
| Certificate Purpose | <p>ドロップダウンリストから必要なオプションを選択します。</p> <p>次のいずれかのオプションを選択すると、[Key Type] フィールドは自動的にRSAに設定されます。</p> <ul style="list-style-type: none"> • Tomcat • IPSec • ITLRecovery • CallManager • CAPF • TVS <p>次のいずれかのオプションを選択すると、[Key Type] フィールドは自動的にEC (楕円曲線) に設定されます。</p> <ul style="list-style-type: none"> • tomcat-ECDSA • CallManager-ECDSA |
| Distribution | ドロップダウンリストから Unified Communications Manager サーバを選択します。 |
| Common Name / Common 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 Common Name_SerialNumber は、証明書のファイル名です。 |
| CSR に OU を含める | <p>デフォルトでは、組織単位フィールドは証明書署名要求から削除されています。証明書署名要求に組織単位フィールドを含めるには、このオプションを選択します。</p> <p>(注) 証明書署名要求に組織単位があり、署名付き CA 証明書にない場合は、署名付き CA 証明書を Unified Communications Manager にアップロードできます。</p> |

| フィールド | 説明 |
|------------------------|---|
| Auto-populated Domains | <p>[証明書の目的 (Certificate by)] ドロップダウンリストを使用して、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。</p> <ul style="list-style-type: none">• tomcat• tomcat-ECDSA• CallManager• CallManager-ECDSA• TVS <p>このフィールドには、1つの証明書によって保護されているホスト名が一覧表示されます。証明書の共通名は、ホスト名と同じです。両方、CALLMANAGER ecdsaとtomcatの両方の証明書には、ホスト名とは異なる共通の名前があります。</p> <p>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。</p> |
| Key Type | <p>このフィールドには、公開キーと秘密キーのペアの暗号化および復号化に使用されるキーのタイプがリストされます。</p> <p>Unified Communications Manager は EC および RSA キー タイプをサポートしています。</p> |

| フィールド | 説明 |
|----------------|---|
| Key Length | <p>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。</p> <ul style="list-style-type: none"> • 1024 • 2048 • 3072 • 4096 <p>キーの長さによっては、自己署名証明書要求によって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を限定して選択した場合は、キー長の強度以上のハッシュアルゴリズム強度を使用できます。</p> <ul style="list-style-type: none"> • キー長の値が256の場合、サポートされているハッシュアルゴリズムは SHA256、SHA384、または SHA512 です。 • キー長の値が384の場合、サポートされているハッシュアルゴリズムは SHA384 または SHA512 です。 <p>(注) キー長の値が3072または4096の証明書は、RSA 証明書に対してのみ選択されます。これらのオプションは、ECDSA 証明書では使用できません。</p> <p>(注) CallManager の [Certificate Purpose] で選択された RSA キー長の値が 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場合があります。</p> <p>詳細については、Cisco Unified Reporting Tool (CURT) の [Unified CM Phone Feature List Report] で、3072/4096 RSA キー サイズ サポート に対応した電話機モデルの一覧を確認できます。</p> |
| Hash Algorithm | <p>ドロップダウンリストからキーの長さ以上の値を選択します。</p> <p>(注)</p> <ul style="list-style-type: none"> • [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基づいて変わります。 • システムが FIPS モードで実行されている場合は、必ずハッシュアルゴリズムとして SHA256 を選択する必要があります。 |

| フィールド | 説明 |
|----------------------------|--|
| Validity Period (in years) | 自己署名証明書の有効期間を設定するには、ドロップダウンリストから [5]、[10]、または [20] などのオプションを選択します。 (注) すべての自己署名証明書のデフォルトの有効期間は 5 年です。 |

証明書の再作成

証明書が期限切れになる前に、証明書を再生成することを推奨します。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 証明書を再作成すると、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。

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) 証明書を再生成する場合、[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 3 [生成 (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。詳細については、「[証明書の名前と説明 \(66 ページ\)](#)」を参照してください。

ステップ 5 CAPF 証明書、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。

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> にある『Cisco Unified Communications Manager セキュリティガイド』を参照してください。

表 12: 証明書の名前と説明

| 名前 | 説明 | 再起動サービス |
|------------------------|---|--|
| tomcat tomcat-ECDSA | この証明書は、SIP Oauth モードが有効な場合に 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。 | (注) 以下のサービスの再起動は、リリース 14 以降に適用されます。 Cisco Tomcat サービス、Cisco Disaster Recovery System (DRS) ローカルおよびマスターサービス、Cisco UDS Tomcat および Cisco AXL Tomcat ウェブサービス。 SAML SSO が Tomcat 証明書で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。 |
| ipsec | この自己署名ルート証明書は、Unified Communications Manager、MGCP、H.323、および IM and Presence サービスとの IPsec 接続のインストール中に生成されます。 | IPsec サービス。 |

| 名前 | 説明 | 再起動サービス |
|--|--|---|
| <p>CallManager CallManager-ECDSA</p> | <p>SIP、SIP トランク、SCCP、TFTP などに使用されます。</p> | <p>(注) リリース 14 の場合、次のサービスを再起動します。 Cisco Call Manager サービスおよびその他の関連サービス (Cisco CTI Manager、HAProxy サービスなど) : サーバーがセキュアモードの場合に CTL ファイルを更新します。</p> <p>(注) 以下のサービスの再起動は、リリース 14 SU1 以降に適用されます。</p> <p>CallManager - HAProxy サービスで、サーバーがセキュアモードの場合は CTL ファイルを更新します。</p> <p>CallManager-ECDSA - Cisco CallManager サービス、HAProxy サービス、TFTP、CTL。</p> |
| <p>CAPF</p> | <p>Unified Communications Manager パブリッシュャで実行されている CAPF サービスで使用されます。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)。</p> | <p>該当なし</p> |
| <p>信頼検証サービス (TVS)</p> | <p>これは信頼検証サービスで使用され、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。</p> | <p>該当なし</p> |



- (注)
- [セキュリティパラメータ (Security Parameter)] セクションには、新しいエンタープライズパラメータとして [証明書更新時の電話機の動作 (Phone Interaction on Certificate Update)] が導入され、TVS、CAPF、TFTP のいずれかの証明書が更新されたときに、電話機のリセットを手動で行うか自動で行うかを設定できます。デフォルトでは、このパラメータは電話機を自動的にリセットするように設定されています。
 - 証明書の再生成、削除、および更新後、「再起動サービス」の列に記載されている適切なサービスを再起動してください。



重要 これは、リリース 14SU2 以降に適用されます。

CLI を使用したマルチ SAN 証明書のアップロードはサポートされていません。これらの証明書は、常に OS 管理 GUI を使用してアップロードする必要があります。

CAPF 証明書の再生成

CAPF 証明書を再生成するには、次の手順を実行します。



- (注) CAPF 証明書がパブリッシュにある場合は、電話機が自動的に再起動して ITL ファイルを更新することがあります。これは、[証明書の更新時の電話の連携 (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。

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、『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。

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。

詳細については、『Cisco Unified Communications Manager セキュリティガイド』の「Activating the Certificate Authority Proxy Function Service」の項を参照してください。

TVS 証明書の再生成



- (注) TV と TFTP の両方の証明書を再生成する場合は、TV 証明書を再生成し、可能な電話機の再起動が完了するまで待ってから、TFTP 証明書を再生成します。これは、[証明書の更新時の電話の連携 (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。

ステップ 1 TVS 証明書の再生成

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、『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。

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

TFTP 証明書の再生成

TFTP 証明書を再生成するには、次の手順を実行します。



- (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。TFTP 証明書を再生成する前に、可能な電話機の再起動が完了するまで待ちます。この手順に従わないと、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生じることがあります。これは、[証明書の更新時の電話の連携 (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。

ステップ 1 TFTP 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 TFTP サービスが有効化されている場合は、すべての電話機が自動的に再起動するまで待ちます。

ステップ 3 クラスタが混合モードの場合は、CTL ファイルを更新します。

ステップ 4 クラスタが EMCC 導入に含まれる場合、証明書の一括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 アドミニストレーションガイド』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 秘密キーです。サーバがクラッシュすると、キーが失われ、電話機は新しい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 証明書と秘密キーの両方がディザスタリカバリシステムによってバックアップされます。システムは、秘密キーの秘密を保持するためにバックアップパッケージを暗号化します。サーバがクラッシュすると、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、新しいシステムの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 この証明書の有効期限が電話機で長いため、ITLRecovery 証明書は頻繁に再生成しないでください。また、この証明書には CallManager 証明書も含まれています。

非セキュアクラスタの ITLRecovery 証明書の再生成

1. ITL ファイルが有効であること、およびクラスタ内のすべての電話機が現在の ITL ファイルを信頼しているかどうかを確認します。
2. ITLRecovery 証明書を再生成します。
各クラスタ内のパブリッシャに移動し、ITLRecovery 証明書を再生成します。
 1. [Unified OS の管理 (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。
[証明書リスト (Certificate List)] ウィンドウが表示されます。
 3. 表示された証明書のリストから、ITLRecovery pem 証明書のリンクをクリックします。
 4. ITLRecovery 証明書を再生成するには、[再生成 (再生成)] をクリックします。
 5. 確認メッセージポップアップで、[OK] をクリックします。
3. CallManager 証明書のユーティリティ `itl reset localkey\` を使用して itl ファイルに署名し、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機を一括してリセットします。



(注) クラスタ内のすべての電話機が登録されていることを確認してください。

5. TFTP サービスを再起動して、新しい ITLRecovery 証明書によって ITL ファイルが再署名されるようにします。

新しい ITLRecovery 証明書は、リセット中に電話機にアップロードされます。

6. クラスタ内のすべての電話機を一括してリセットし、新しい ITL ファイルを取得します。
7. リセット後に、新しい ITLRecovery 証明書を使用して電話機がアップロードされます。

セキュアクラスタの ITLRecovery 証明書の再生成

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「migration」の項を参照してください。

1. ITL ファイルが有効であることと、クラスタ内のすべての電話機が現在の ITL ファイルを信頼していることを確認します。

2. `show ctl` コマンドを使用して `ctl` ファイルを確認します。

3. ITLRecovery 証明書を再生成します。

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

1. [Unified OS の管理 (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. [検索 (Find)] をクリックして、証明書の一覧を表示します。

[証明書リスト (Certificate List)] ウィンドウが表示されます。

3. 表示された証明書のリストから、ITLRecovery pem 証明書のリンクをクリックします。

4. ITLRecovery 証明書を再生成するには、[再生成 (再生成)] をクリックします。

5. 確認メッセージポップアップで、[OK] をクリックします。

4. CallManager 証明書で、CTLFile にユーティリティ `ctl reset localkey\` を使用して署名します。これにより、新しい ITLRecovery 証明書を使用して CTLFile も更新されます。

5. クラスタ内のすべての電話機を一括してリセットし、新しい ITLRecovery 証明書を使用して新しい CTLFile をピックアップします。



- (注)
- クラスタ内のすべての電話機が登録済みであることを確認してください。
 - ITLRecovery を再生成すると、システム全体の証明書が有効化に使用される場合、クラスタの SAML SSO ログインに影響します。

6. 新しい ITLRecovery Certificate CTLFile `ctl Update CTLFile` によって再署名されるように、を更新します。

7. クラスタ内のすべての電話機を一括してリセットし、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. リセット後、新しい ITLRecovery 証明書が電話機にアップロードされます。

tomcat 証明書の再生成



(注) リリース 14 以降では、SIP OAuth が有効になっている場合、Tomcat の再起動後に SIP OAuth を使用するように設定された電話機を手動でリセットする必要があります。

Tomcat 証明書を再生成するには、次の手順を実行します。

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 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 3 クラスタが EMCC 導入に含まれる場合、証明書の一括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 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、パブリッシュノードの 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 (Security)] > [証明書の管理 (Certificate Management)] を選択し、AUTHZ 証明書を選択して、[再作成 (Regenerate)] をクリックします。

ステップ 1 Unified Communications Manager パブリッシャノードで、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 サービスのローカル 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) 次のシナリオでは、Cisco XCP 認証サービスを再起動する必要があります。

- Authz 証明書を再生成する場合
- IM and Presence e管理コンソールで集中型展開に新しいエントリを作成する場合

信頼ストアへの認証局署名済み CAPF ルート証明書の追加

認証局署名済み CAPF ルート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。

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 (Upload Certificate/Certificate chain)] 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 (Upload Certificate/Certificate chain)] ポップアップウィンドウで、[証明書の目的 (Certificate Purpose)] ドロップダウンリストから [CallManager-trust] 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 (Upload File)] フィールドに証明書が表示されたら、[アップロード (Upload)] 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 コマンドを使用して 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は、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。

ステップ 1 Unified Communications Manager のパブリッシュノードから、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 ctl update CTLfile` コマンドを実行します。CTL ファイルを再生成すると、ファイルが TFTP サーバにアップロードされて、電話機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** をサポートしない SIP デバイスは、引き続き **TLS_ECDHE_RSA_WITH_AES_256_SHA384**、**TLS_ECDHE_RSA_WITH_AES_128_SHA256**、または **AES128_SHA**。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 only**] オプションを選択した場合、**ecdsa** 暗号をサポートしていないデバイスは、SIP インターフェイスへの TLS 接続を確立できません。[**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** と **TLS_ECDHE_ECDSA_WITH_AES256_SHA384** になります。
- CTI Manager 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。ただし、**AES128_SHA** を使用して接続できます。
- Unified Communications Manager は、同じ SubjectDN を持つ複数の証明書を同じ信頼ストアにアップロードすることをサポートしていません。サーバーが新しい証明書と既存の証明書を区別するために、ユーザーは新しい CN を別の名前で使用するか、SubjectDN-issue-CA-G2 または SubjectDN-issue-CA-2023 のように文字をサフィックスとして使用することをお勧めします。ハッシュリンクも同じように作成されます。

証明書のモニタリングと失効タスクのフロー

このセクションでは、更新が必要な証明書をモニタし、有効期限が切れた証明書を無効にできます。

証明書モニタリングの概要

管理者は、自動化されたシステムが Unified Communications Manager および IM and Presence Service サービスに含まれている場合、証明書を追跡および更新する必要があります。証明書モニタリングは、管理者が証明書のステータスを継続的に知り、証明書の有効期限が近づいたときに電子メールで通知を受信するのに役立ちます。

証明書モニタリングの設定

Cisco Certificate Expiry Monitor ネットワークサービスが実行されている必要があります。このサービスはデフォルトで有効になりますが、Cisco Unified Serviceability でサービスが実行されていることを確かめるには、[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)] のステータスが [実行中 (Running)] であることを確認します。

ステップ 1 Cisco Unified OS Administration で、[セキュリティ (Security)] > [証明書モニタ (Certificate Monitor)] を選択します。

ステップ 2 設定の詳細を入力または選択します。

ステップ 3 [保存 (Save)] をクリックして、設定を保存します。

(注) デフォルトで、証明書モニタサービスは 24 時間ごとに 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。証明書の有効期限が 7 日以内に近づいても、この頻度は変わりません。このサービスは、証明書の有効期限が切れる 1 日前から、有効期限が切れた後も 1 時間おきに実行します。

証明書失効の概要

このセクションでは、証明書失効について説明します。Cisco UCM は、証明書失効をモニタするためにオンライン証明書ステータスプロトコル (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るたびに、スケジュールされたタイムラインで、システムはそのステータスをチェックして有効性を確認します。

コモンクライテリアモードが有効になっている FIPS 展開の場合、OCSP はシステムのコモンクライテリア要件への準拠にも役立ちます。

証明書失効の設定

[有効性検証 (Validation Checks)] では、Unified Communications Manager は証明書のステータスを確認し、有効性を確認します。

証明書の検証手順は次のとおりです。

- Unified Communications Manager は代理信頼モデル (DTM) を使用し、OCSP 署名属性のルート CA または中間 CA をチェックします。ルート CA または中間 CA は、OCSP 証明書に署名してステータスを確認する必要があります。
- 代理信頼モデルが失敗した場合は、レスポンドの信頼モデル (TRP) に戻ります。次に、Unified Communications Manager は OCSP サーバからの指定された 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には、OCSP 応答側が実行されている必要があります。

期限切れの証明書が自動的に失効するように OCSP を設定します。[証明書失効 (Certificate Revocation)] ウィンドウで OCSP オプションを有効にすると、最も安全な方法でリアルタイムに証明書失効をチェックすることができます。オプションから、証明書の OCSP URI を使用するか、または設定済みの OCSP URI を使用するかを選択します。



(注) syslog、FileBeat、SIP、ILS、LBM など、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ます。OCSP 応答属性で設定されたルート CA 証明書または中間 CA 証明書、または tomcat-trust にアップロードされた、指定 OCSP 署名証明書を使用できます。



重要 このセクションは、リリース 14SU3 以降に適用されます。

証明書失効は、無効で信頼できない証明書を、信頼できる有効な証明書と区別するプロセスです。CA が 1 つ以上のデジタル証明書が信頼できなくなったことを通知し、期限日の前に証明書を本質的に無効にする場合。

証明書失効リスト (CRL) は、実際の期限日または割り当てられた期限日の前に認証局によって失効されたデジタル証明書のリストです。証明書失効リストは、Public Key Infrastructure (PKI) と Web セキュリティに不可欠です。すべての CA には、独自の CRL リストがあります。

この機能は主に CA 発行の CAPF 署名付き電話 LSC 向けに設計されています。CA からダウンロードした最新の CRL ファイルと以前にダウンロードした CRL ファイルに相違がある場合は常に、*CRLChanged* アラームが生成され、syslog のメッセージとともに RTMT に表示されます。*CRLChanged* アラームの詳細については、Cisco Unified Real-Time Monitoring Tool を確認してください。

管理者は、有効な証明書チェーンを更新して置き換えることでアラームに対処し、CallManager で影響を受けるサービスを再起動して、取り消された証明書を使用していた既存の TLS 接続を終了する必要があります。その後、有効な新しい証明書を使用して新しい接続が確立されます。

- 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** [ANATの有効化 (Enable OCSP)] チェックボックスを選択します。
- ステップ 3** 証明書に OCSP レスポンダ URI が設定されている場合は、[証明書からの OCSP URI を使用する (Use OCSP URI from Certificate)] 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、[設定された OCSP URI を使用 (Use Configured OCSP URI Option)] をクリックします。
- ステップ 5** レスポンダの [OCSP の設定済み URI] を入力します。
- ステップ 6** 失効チェックを有効にするには、[失効チェックの有効化 (Enable Revocation Check)] チェックボックスをオンにします。
- ステップ 7** 失効ステータスを確認する頻度を入力し、[時間 (Hours)] または [Days (日)] から時間間隔をクリックします。
- ステップ 8** [CRL有効化 (Enable CRL)] チェックボックスをオンにします。
- ステップ 9** CRL ファイルのダウンロード元の **CRL 配布ポイント URI** を入力します。
- ステップ 10** [保存 (Save)] をクリックします。

(注) シスコ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求める、アラートがポップアップ表示されます。このポップアップは、[OCSPの有効化 (Enable OCSP)] チェックボックスをオンにした場合、または以降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、検証とコモンクライテリア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。

- [良好 (Good)] : OCSP レスポンダがステータスの照会に対して肯定的な応答を送信していることを示します。証明書は失効しませんが、証明書が発行されたという意味でも、応答時間が証明書の有効期間内にあるという意味でもありません。Response 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レスポンドが行ったより多くの要求を伝えます。
- [失効 (Revoked)] : 証明書が永久的または一時的に失効 (保留) ステータスにあることを示します。
- [不明 (Unknown)] : OCSP レスポンダが要求された証明書について認識していないことを示しています。

警告 コモンクライテリアモードを有効にした場合、接続は [失効済み (Revoked)] および [不明 (Unknown)] のケースで失敗します。コモンクライテリアモードを無効にすると、接続は [不明 (Unknown)] のケースで成功します。

- ステップ 11** (任意) CTI、IPsec または LDAP リンクがある場合は、これらの長期的に中断しない接続の 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 (System)] > [エンタープライズパラメータ (Enterprise Parameters)] を選択します。
 - b) [証明書失効と有効期限 (Certificate Revocation and Expiry)] ペインに移動します。

- c) [証明書有効性チェック (Certificate Validity Check)] パラメータを [有効 (Enabled)] に設定します。
- d) [有効性チェック頻度 (Validity Check Frequency)] パラメータの値を入力します。
 - (注) [証明書失効 (Certificate Revocation)] ページの [失効チェックの有効化 (Enable Revocation Check)] パラメータの間隔値は、[有効性チェックの頻度 (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。

簡素化された証明書管理

更新プログラムのコレクションにより、管理する必要がある証明書の数が大幅に削減されるため、証明書の要件を満たすことが容易になります。Unified Communications Managerには8つのアイデンティティ証明書があります。各ノードの CallManager、CallManager-ECDSA、Tomcat、Tomcat-ECDSA、IPsec、CAPF、TVS、ITL Recoveryです。これらの証明書は、有効期間に基づいて定期的に更新する必要があります。したがって、マルチクラスタ展開シナリオでは、これらの証明書を管理することは困難です。

簡略化された証明書管理の概要

証明書を効率的に管理するには、証明書の数を減らして再利用するオプションがあります。

- **TVS によるマルチサーバ SAN 証明書のサポート** : TVS は、自己署名オプションと CA 署名オプションの両方でマルチサーバ SAN 証明書をサポートするようになり、クラスタに単一の証明書を導入できるようになりました。これらの証明書はクラスタベースです。各クラスタには、ITL ファイルサイズと管理オーバーヘッドを削減する TVS 証明書を1つだけ持つオプションがあります。たとえば、21のノードがある場合、各クラスタに必要な証明書は1つだけです。
- **パブリッシャノードから生成された CAPF 証明書** : CAPF 証明書がパブリッシャノードからのみ生成されるようになり、クラスタに単一の証明書を展開できるようになりました。ただし、CAPF 証明書は、エンドポイント登録用のパブリッシャノードとサブスクリバノードの両方で信頼証明書 (Callmanager-trust) として使用できます。
- **マルチサーバ SAN 自己署名証明書のサポート** : Tomcat、Tomcat-ECDSA、CallManager、CallManager-ECDSA 証明書は、マルチサーバ SAN 自己署名証明書をサポートするようになりました。以前は、マルチサーバ SAN 証明書は CA 署名付き証明書でのみサポートされていました。マルチサーバ SAN 自己署名証明書を使用することで、サードパーティ認証局から CA を管理するコストを回避できるようになりました。
- **CallManager にマルチサーバ Tomcat 証明書を再利用する** : CallManager 証明書にマルチサーバ Tomcat 証明書を再利用できるようになりました。これは、それぞれに個別の証明書を生成する必要がないためです。CallManager 証明書にマルチサーバ Tomcat 証明書を再

利用する方法の詳細については、「[CallManager 用のマルチサーバ Tomcat 証明書の再利用 \(80 ページ\)](#)」を参照してください。

- **自己署名証明書の有効期間**：自己署名証明書のデフォルトの有効期間が短縮されます。有効期間を短縮することで、キーは短い期間で定期的に更新され、古い証明書が削除されます。証明書の有効期間が長いほど、秘密キーが侵害される可能性が高くなります。すべての自己署名証明書のデフォルトの有効期間は 5 年です。

[**有効期間 (Validity Period)**] フィールドを使用して、自己署名証明書の有効期間を設定するオプションもあります。詳細については、[自己署名証明書の生成](#) セクションを参照してください。

表 13: Cisco Unified Communications Manager CSR キーの用途拡張

| 証明書 | Unified CM リリース 14 以前 | | | | Unified CM リリース 14 以降 | | | |
|-------------------|-----------------------|-----------------------|-----------------------|--------------|-----------------------|-------------------|-----------------------|---------------|
| | マルチサーバ SAN 自己署名をサポート | マルチサーバ SAN CA 署名をサポート | 10 ノードクラスターで管理する証明書の数 | ノード/クラスターベース | マルチサーバ SAN 自己署名をサポート | マルチサーバ CA 署名をサポート | 10 ノードクラスターで管理する証明書の数 | ノード/クラスターベース |
| Tomcat | N | Y | 1 | 自己署名時のノードベース | Y | Y | 1 | Cluster-based |
| Tomcat-ECDSA | N | Y | 1 | 自己署名時のノードベース | Y | Y | 1 | Cluster-based |
| CallManager | N | Y | 1 | 自己署名時のノードベース | Y | Y | 0 | Cluster-based |
| CallManager-ECDSA | N | Y | 1 | 自己署名時のノードベース | Y | Y | 0 | Cluster-based |
| 信頼検証サービス (TVS) | N | N | 10 | ノードベース | Y | Y | 1 | Cluster-based |
| CAPF | N | N | 10 | ノードベース | Y | N | 1 | バブリッシュャでのみ |
| IPsec | N | N | 10 | ノードベース | N | N | 0 | ノードベース |
| ITLRecovery | N | N | 1 | ノードベース | N | N | 1 | Cluster-based |

簡素化された証明書管理ユーザインターフェイスの更新

次のユーザインターフェイスの更新が導入されました。

- **[証明書の再利用 (Reuse Certificate)]**：[証明書管理 (Certificate Management)] ウィンドウには、Tomcat マルチサーバ証明書を CallManager アプリケーションと共有できるこの新しいオプションがあります。これにより、ITL ファイルのサイズが削減され、オーバーヘッドが削減されます。
- **[証明書の表示 (Show Certificates)]**：Cisco Unified OS の管理インターフェイスの [証明書の管理 (Certificate Management)] ウィンドウには、アイデンティティと信頼の証明書のリストを表示できる新しいフィルタリングオプションがあります。

CallManager 用のマルチサーバ Tomcat 証明書の再利用

CallManager アプリケーションで Tomcat マルチサーバ証明書を再利用できるようになりました。CA から 1 つの証明書を取得し、アプリケーション間で再利用できます。これにより、管理オーバーヘッドとコストの最適化が削減されます。



(注) Tomcat 証明書を再利用する前に、マルチサーバ SAN サポート証明書であることを確認してください。

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 [証明書の再利用 (Reuse Certificate)] をクリックします。

[他のサービスに Tomcat 証明書を使用する] ページが表示されます。

ステップ 3 [Tomcat タイプの選択] ドロップダウンリストから、[tomcat] または [tomcat-ECDSA] を選択します。

ステップ 4 [次の証明書を置き換える] ペインで、[CallManager] または [CallManager-ECDSA] チェックボックスをオンにします。

ステップ 5 CallManager 証明書を tomcat マルチサーバ SAN 証明書に置き換えるには、[終了 (Finish)] をクリックします。

- (注)
- 証明書タイプとして tomcat を選択すると、CallManager が置換として有効になります。
 - 証明書タイプとして tomcat-ECDSA を選択すると、置換として CallManager-ECDSA が有効になります。
-



第 6 章

Certificate Authority Proxy Function

- 認証局プロキシ機能の概要 (81 ページ)
- 認証局プロキシ機能の設定タスクフロー (83 ページ)
- 認証局プロキシ機能の管理タスクフロー (92 ページ)
- CAPF システムの連携動作 (95 ページ)

認証局プロキシ機能の概要

認証局プロキシ機能 (CAPF) は、ローカルで重要な証明書 (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 上で実行され、次のタスクを実行します。

- サポートされる Cisco Unified IP Phone に LSC を発行します。
- 混合モード中に電話機を認証します。
- 電話機用の既存の LSC をアップグレードする。
- 表示とトラブルシューティングのために電話機証明書を取得する。

CAPF サービス証明書

CAPF サービスは Unified Communications Manager のインストールで自動的にインストールされ、CAPF 固有のシステム証明書が生成されます。

これは、リリース 14 SU2 以降に適用されます。



(注) CAPF 証明書には、次のデフォルトの X509 拡張を含める必要があります。

X509v3 基本制約 :

CA:TRUE, pathlen:0

X509v3 キーの用途 :

デジタル署名、証明書署名

CAPF 証明書にこれらの拡張機能がない場合、TLS 接続が失敗します。

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 14: CAPF 実行モード

| モード | 説明 |
|--------------------------------|---|
| Cisco Authority Proxy Function | デフォルトでは、Unified Communications Manager 上の CAPF サービスが、CAPF サービスで署名された LSC を発行します。 |
| オンライン 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。CA 署名 LSC は、証明書署名要求 (CSR) が送信されると自動的に返されます。 |
| オフライン 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。SC を手動でダウンロードして CA に提出し、CA 署名の証明書の準備ができてからそれらをアップロードします。 (注) LSC の署名にサードパーティ CA を使用する場合は、[オフライン CA (Offline CA)] ではなく [オンライン CA (Online CA)] オプションをお勧めします。[オンライン CA (Online CA)] は自動化されていて、はるかに速く、問題が発生する可能性が低いです。 |

LSC を生成する前に、次のものを用意していること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 (Cisco Unified IP Phone および Jabber を含む)。
- 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、電話機を認証する方法も決定します。

LSC を生成する前に、CA ルート証明書と HTTPS 証明書を必要な信頼ストアに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 接続では、HTTPS 証明書は CAPF-トラストを通過し、CA ルート証明書は CAPF 信頼と Unified Communications Manager 信頼の両方を通過します。CA ルート証明書は、証明書署名要求 (CSR) への署名に使用されます。

次に、さまざまな証明書をアップロードするシナリオを示します。

表 15: 証明書のアップロードシナリオ

| シナリオ | アクション |
|---|-------------------------------|
| CA ルート証明書と HTTPS 証明書が同じ。 | CA ルート証明書をアップロードする。 |
| CA ルート証明書と 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 証明書と 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。 |
| 同じ CA ルート証明書が、異なる CA ルート証明書と HTTPS 証明書を発行します。 | CA ルートおよび HTTPS 証明書をアップロードする。 |



(注) 複数の証明書を同時に生成すると、コールプロセスが中断され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 を使用することをお勧めします。

認証局プロキシ機能の設定タスクフロー

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。



(注) 新しい CAPF 証明書を再生成またはアップロードした後に、CAPF サービスを再起動する必要はありません。

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。その他の場合は、このタスクをスキップします。 |
| ステップ 2 | 認証局 (CA) ルート証明書のアップロード (85 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 (86 ページ) | 電話機の 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 サービスのアクティブ化または再起動 | CAPF システム設定を構成した後、必須の 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 で CAPF 設定を構成します。 <ul style="list-style-type: none"> ユニバーサルデバイステンプレートでの CAPD 設定の構成 (89 ページ) 一括管理による CAPF 設定の更新 (90 ページ) 電話機の CAPF 設定の構成 (91 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。 <ul style="list-style-type: none"> 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します。 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 (92 ページ) | ファイアウォールがタイムアウトしないように、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、外部 CA を使用して LSC 証明書に署名します。



(注) LSC の署名にサードパーティ CA を使用しない場合は、このタスクをスキップします。

- ステップ 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。
- ステップ 2 [証明書/証明書チェーンのアップロード (Upload Certificate/Certificate chain)] 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、[CAPF 信頼 (CAPF-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 の証明書のように指定します。
- 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、[証明書の用途 (Certificate Purpose)] を [CallManager 信頼 (callmanager-trust)] として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-」サブストリングが含まれていないことを確認します。「CAPF-」共通名は、CAPF 証明書用に予約されています。

- 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 (Upload Certificate/Certificate chain)] 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、[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 の証明書のように指定します。
- 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。

重要 これは、リリース 14 SU2 以降に適用されます。

- (注) ルートまたは中間 CA 証明書には、次のデフォルトの X509 拡張を含める必要があります。

X509v3 基本制約 :

CA:TRUE, pathlen:0

X509v3 キーの用途 :

デジタル署名、証明書署名

証明書にこれらの拡張機能がない場合、TLS 接続が失敗します。

重要 この注記は、リリース 14 SU3 以降の IPsec 証明書にのみ適用されます。

(注) CA 署名付き IPsec 証明書には、次の拡張子を含めないでください。

X509v3 基本制約 :

CA:TRUE

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 でこの手順を使用します。

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 (Server)] ドロップダウンリストから、[Cisco Certificate Authority Proxy Function (アクティブ) (Cisco Certificate Authority Proxy Function (Active))] サービスをアクティブにしたノードを選択します。

ステップ 3 [サービス (Service)] ドロップダウンリストで、[Cisco 証明書認証プロキシ機能 (アクティブ) (Cisco Certificate Authority Proxy Function (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 署名付き証明書の場合、オンライン CA を使用することを推奨します。

ステップ 5 [証明書の有効期間 (日数) (Duration Of Certificate Validity (in Days))] 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 (Online CA Parameters)] 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 (Online CA Hostname)] : 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 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る HTTPS 証明書の共通名 (CN) と同じです。

- [オンライン CA ポート (Online CA Port)] : オンライン CA のポート番号を入力します。たとえば、443 のように指定します。

- [オンライン CA テンプレート (Online CA Template)] : 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。

(注) このフィールドは、[オンライン CA タイプ (Online CA Type)] が [Microsoft CA] のときのみ有効です。

- [オンライン CA タイプ (Online CA Type)] : エンドポイント証明書の自動登録には、Microsoft CA または EST でサポートされる CA を選択します。

- [Microsoft CA] : CA が Microsoft CA である場合、このオプションを使用して、デジタル証明書をデバイスに割り当てます。

(注) FIPSS 対応モードは、Microsoft CA ではサポートされていません。

- **重要** リリース 14SU2 以降でサポートされます。

[EST サポート CA (EST Supported CA)] : CA が自動登録用の組み込み EST サーバーモードをサポートしている場合は、このオプションを使用します。

- [オンラインCAユーザ名 (Online CA Username)] : 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 (Online CA Password)] : CA サーバのユーザ名のパスワードを入力します。
- [証明書登録プロファイルラベル (Certificate Enrollment Profile Label)] : EST がサポートする CA のデジタル ID を有効な文字で入力します。

(注) このフィールドは、[オンライン CA タイプ (Online CA Type)] が [EST サポート CA (EST Supported CA)] の場合にのみ有効です。

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 (Save)] 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 Certificate Authority Proxy Function** を再起動します。Cisco Certificate Enrollment サービスが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。
- 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」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、手動による手順が非常に多くなります。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。

- 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** ルート証明書チェーンを Unified Communications Manager 内の必要な信頼（CallManager 信頼 CAPF 信頼）にアップロードします。
- ステップ 3** [エンドポイントへの証明書の発行（Certificate Issue to Endpoint）] サービスパラメータを [オフライン CA（Offline CA）] に設定して、オフライン CA を使用するように Unified Communications Manager を設定します。
- 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 署名済み LSC の作成およびインポートの設定](#)」を参照してください。

CAPF サービスのアクティブ化または再起動

CAPF システム設定を構成した後、必須の 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。

- ステップ 1** Cisco Unified Serviceability から、[ツール（Tools）]>[サービスアクティベーション（Service Activation）] 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ュノードを選択し、[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（Security Services）] ペインで、適用され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、このサービスをオンにし、そうでない場合はオフのままにします。
 - **Cisco Certificate Authority Proxy Function** : オフになっている（非アクティブ）場合は、このサービスをオンにします。この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** 設定を編集した場合は、[保存（Save）] をクリックします。
- ステップ 5** **Cisco Certificate Authority Proxy Function** 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（Related Links）] ドロップダウンリストから [コントロールセンター - 機能サービス（Control Center - Feature Services）] を選択し、[移動（Go）] をクリックします。

- b) [セキュリティ設定 (Security Settings)] ペインで、[Cisco Certificate Authority Proxy Function] サービスをオンにして、[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) [ユニバーサル デバイス テンプレートでの CAPD 設定の構成 \(89 ページ\)](#)
- b) [一括管理による CAPF 設定の更新 \(90 ページ\)](#)
- c) [電話機の CAPF 設定の構成 \(91 ページ\)](#)

ユニバーサル デバイス テンプレートでの CAPD 設定の構成

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することができます。テンプレートの CAPF 設定は、このテンプレートを使用する同期のすべてのデバイスに適用されます。



(注) ユニバーサル 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、「[一括管理による CAPF 設定の更新 \(90 ページ\)](#)」を参照してください。

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 (Find)] をクリックして、既存のテンプレートを選択します。
- [新規追加 (Add New)] 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 (Certificate Authority Proxy Function (CAPF) Settings)] 領域を展開します。

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 (Authentication Mode)] ドロップダウンリストメニューから、デバイスを認証するための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、[認証文字列 (Authentication String)] テキストボックスに文字列を入力するか、または [文字列を生成 (Generate String)] 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 (Save)] 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式で設定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 次の手順に従って、このプロファイルを使用しているデバイスにテンプレートの設定を適用します。

- a) ユニバーサル デバイス テンプレートを [機能グループテンプレートの設定 (Feature Group Template Configuration)] に追加します。
- b) 同期されていない LDAP ディレクトリ設定に機能グループテンプレートを追加します。
- 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「エンドユーザの設定」の項を参照してください。

一括管理による CAPF 設定の更新

Bulk Administrationの電話機の更新クエリを使用して、1回の操作で多数の既存の電話機にCAPF設定とLSC証明書を設定します。



- (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 (Insert phone)]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文字列と認証方式と同じ文字列と認証方式で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、電話ドキュメンテーションを参照してください。

ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[一括管理 (Bulk Administration)] > [電話機 (Phones)] > [電話機の更新 (Update Phones)] > [クエリ (Query)]

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 (Find)] をクリックします。

たとえば、[電話機の検索場所 (Find phones where)] ドロップダウンリストを使用して、特定の日付の前にLSCの有効期限が切れる電話機や、特定のデバイスプールにある電話機をすべて選択します。

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/リスタート (Logout/Reset/Restart)] セクションで、[設定の適用 (Apply Config)] ラジオボタンを選択します。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** [認証局プロキシ機能 (CAPF) 情報 (Certification Authority Proxy Function (CAPF) Information)] 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 (Certificate Operation)] 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 (Install/Upgrade)] 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 (Authentication Mode)] ドロップダウンリストから、LSC の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式を設定します。
- ステップ 8** [認証モード (Authentication Mode)] として [認証文字列による (By Authentication String)] を選択した場合は、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 (Generate unique authentication string for each device)] をオンにします。
 - 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 (Authentication String)] テキストボックスに文字列を入力するか、[文字列の生成 (Generate String)] をクリックします。
- ステップ 9** [電話の更新 (Update Phones)] ウィンドウの [認証局プロキシ機能 (CAPF) 情報 (Certification Authority Proxy Function (CAPF) Information)] セクションで、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 (Run Later)] 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 (Apply Config)] オプションを選択しなかった場合は、[電話機の設定 (Phones Configuration)] ウィンドウですべての更新された電話機に設定を適用します。

電話機の CAPF 設定の構成

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) LDAP 設定を多数の電話機に適用するには、一括管理または CAPF ディレクトリ同期を使用します。

この手順で追加するのと同じ文字列と認証方式で電話機を設定します。それ以外の場合、電話機は CAPF に対してそれ自体を認証しません。電話機で認証を設定する方法の詳細については、電話ドキュメンテーションを参照してください。

-
- ステップ 1** [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[デバイス (Device)] > [電話 (Phone)]
- 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。[電話の設定 (Phone Configuration)] 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) 情報 (Certification Authority Proxy Function (CAPF) Information)] ペインに移動します。
- ステップ 4** [証明書の操作 (Certificate Operation)] 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 (Install/Upgrade)] 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 (Authentication Mode)] ドロップダウンリストから、LSC の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、同じ認証方式を使用するように設定する必要があります。
- ステップ 6** [認証文字列による (By Authentication String)] を選択した場合は、テキスト文字列を入力するか、[文字列の生成 (Generate String)] をクリックして文字列を生成します。
- ステップ 7** [電話の設定 (Phone Configuration)] ページの [認証局プロキシ機能 (CAPF) 情報 (Certification Authority Proxy Function (CAPF) Information)] ペインで、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。

-
- ステップ 1** コマンドラインインターフェイスを使用して、パブリッシャノードにログインします。
- 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、**Enter** キーを押します。
-

認証局プロキシ機能の管理タスクフロー

CAPF を設定して LSC 証明書を発行したら、LSC 証明書を継続的に管理します。

手順

| | コマンドまたはアクション | 目的 |
|--------|-----------------|---|
| ステップ 1 | CAPF 経由の LSC 生成 | CAPF を設定した後、設定されている認証文字列を電話機に追加します。キーと証明書の交換は、電話機と CAPF の間で行われます。 |
| ステップ 2 | 古い LSC レポートの実行 | Cisco Unified Reporting から古い LSC レポートを実行します。古い LSC 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 LSC がインストールされる前に新しい CSR がエンドポイントにより生成されたため、インストールされません。 |
| 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 ユニファイドレポートから実行します。古い LSC とは、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、その LSC がインストールされる前にエンドポイントによって新しい CSR が生成されたため、インストールされなかったものです。



(注) パブリッシャーノードで `utils capf stale-lsc list` CLI コマンドを実行して、古い LSC 証明書のリストを取得することもできます。

ステップ 1 Cisco Unified Reporting から、[システムレポート (System Reports)] を選択します。

ステップ 2 左側のナビゲーションバーで、[古い LSC (Stale LSCs)] を選択します。

ステップ 3 [新規レポートの生成 (Generate a new report)] 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、以下が発生します。

- 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) キーの生成を低い優先順位で設定すると、アクションの発生中に、電話機が機能します。電話機は証明書生成中に機能しますが、TLS トラフィックが追加された場合、電話機でのコールプロセスの中断が最小限に抑えられ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。

ステップ 1 コマンドラインインターフェイスを使用して、パブリッシャノードにログインします。

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。

ステップ 1 コマンドラインインターフェイスを使用して、パブリッシャノードにログインします。

ステップ 2 `utils capf stale-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 システムの連携動作

表 16: CAPF システムの連携動作

| 機能 | 連携動作 |
|--|---|
| 認証文字列 | CAPF 認証方式での操作の後、電話機で同じ認証文字列を入力します。そうでない場合、操作が失敗します。[TFTP 暗号化設定 (TFTP Encrypted Config)] エンタープライズパラメータが有効な状態で認証文字列の入力に失敗した場合、電話の設定は失敗し、該当する認証文字列が電話に入力されるまで回復しません。 |
| 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で、同じ管理者ユーザ名とパスワードを使用する必要があります。これにより、CAPF でクラスタ内のすべてのサーバを認証することができます。 |
| セキュアな電話機の移行 | <p>セキュアな電話機が別のクラスタに移動した場合、LSC 証明書が CTL ファイルにない別の CAPF により発行されているため、Unified Communications Manager は電話機が送信した LSC 証明書を信頼しません。</p> <p>セキュアな電話を登録可能にするには、既存の CTL ファイルを削除します。その後、[インストール/アップグレード (Install/Upgrade)] オプションを使用して新しい CAPF により新規 LSC 証明書をインストールし、新しい CTL ファイルのために電話をリセットします (または MIC を使用します)。電話を移動する前に、[電話の設定 (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、既存の LSC を削除します。</p> |
| Cisco Unified IP 電話 6900、7900、8900、および 9900 シリーズ | <p>今後の互換性の問題を回避するために、Cisco Unified IP Phone 6900、7900、8900、および 9900 シリーズをアップグレードして、Unified Communications Manager への TLS 接続に LSC を使用し、Unified Communications Manager 信頼ストアから MIC ルート証明書を削除することをお勧めします。Unified Communications Manager への TLS 接続に MIC を使用する一部の電話機モデルでは、登録できない場合があります。</p> <p>管理者は Unified Communications Manager 信頼ストアから次の MIC ルート証明書を削除する必要があります。</p> <ul style="list-style-type: none"> • CAP-RTP-001 • CAP-RTP-002 • Cisco_Manufacturing_CA • Cisco_Root_CA_2048 |

| 機能 | 連携動作 |
|---------|--|
| 停電 | <p>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。</p> <ul style="list-style-type: none"> 電話機は、電話機への証明書のインストール中に通信障害が発生した場合に、30 秒の間隔で 3 回証明書の取得を試行します。これらの値をユーザが設定することはできません。 電話機が CAPF とのセッションを試行している間に電源が故障した場合、電話機はフラッシュに保存された認証モードを使用します。電話機が TFTP サーバから新しい設定ファイルを読み込めない場合、システムはフラッシュ値をクリアします。 |
| 証明書の暗号化 | <p>Unified Communications Manager リリース 11.5(1) SU1、SHA-256 アルゴリズム署名以降、すべての LSC 証明書は CAPF サービスによって発行されます。したがって、IP 電話 7900/8900/9900 シリーズのモデルは、SHA-256 署名済み LSC 証明書および外部 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。</p> <p>(注) 電話機を使用する場合は、ソフトウェア保守の最後にある電話機モデル、またはサポート終了モデルには、Unified Communications Manager 11.5(1) SU1 リリースより前のを使用することをお勧めします。</p> |

7942 および 7962 電話機での CAPF の例

ユーザまたは Unified Communications Manager が電話機をリセットする際に、CAPF が Cisco Unified IP Phone 7962 および 7942 と相互に作用する方法を検討してください。



(注) この例で、CAPF 証明書操作は、LSC が電話機に存在しない場合に、[CAPF 認証モード (CAPF Authentication Mode)] に [既存の証明書 (By Existing Certificate)] を選択すると失敗します。

例：非セキュア デバイス セキュリティ モード

この例では、[デバイスセキュリティ モード (Device Security Mode)] を [非セキュア (Nonsecure)] に設定し、[CAPF 認証モード (CAPF Authentication Mode)] を [Null 文字列 (By Null String)] または [既存の証明書 (優先) (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、構成ファイルを受信します。その後、電話機は CAPF とのセッションを自動的に開始して LSC をダウンロードします。ダウンロードした LSC を電話にインストールした後、[デバイスセキュリティモード (Device Security Mode)] を [認証済み (Authenticated)] または [暗号化 (Encrypted)] 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、[デバイス セキュリティ モード (Device Security Mode)] を [認証済み (Authenticated)] または [暗号化 (Encrypted)] に設定し、[CAPF 認証モード (CAPF Authentication Mode)] を [NULL 文字列 (By Null String)] または [既存の証明書 (優先) (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て電話機が LSC をインストールするまで、電話機はプライマリ Unified Communications Manager に登録しません。セッションが終了すると、電話機が登録され、すぐに認証モードまたは暗号化モードで実行されます。

この例では、電話機が CAPF サーバに自動的に接続しないため、[認証文字列 (By Authentication String)] を設定することはできません。電話機に有効な LSC が存在しない場合、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、または両方のタイプのアドレスを使用する電話機に証明書を発行し、アップグレードします。IPv6 アドレスを使用する SCCP が実行されている電話機に対して証明書を発行またはアップグレードするには、Cisco Unified Communications Manager Administration で [IPv6 の有効化 (Enable IPv6)] サービスパラメータを [True] に設定する必要があります。

CAPF では [Enable IPv6 (IPv6 の有効化)] エンタープライズパラメータの設定を使用して、その電話機への証明書の発行またはアップグレードを実行します。このエンタープライズパラメータが [False] に設定された場合、CAPF は IPv6 アドレスを使用する電話機からの接続を無視または拒否し、その電話機は証明書を受け取りません。

次の表では、IPv4、IPv6、または両方のタイプのアドレスを持つ電話機が CAPF に接続する方法について説明します。

表 17: IPv6 または IPv4 電話機の CAPF への接続方法

| 電話機の IP モード | 電話機の IP アドレス | CAPF IP アドレス | 電話機から CAPF への接続方法 |
|-------------|-------------------|--------------|--|
| 2 スタック | IPv4 と IPv6 が利用可能 | IPv4、IPv6 | 電話機は、IPv6 アドレスを使用して CAPF に接続します。電話機は、IPv6 アドレスを介して接続できない場合、IPv4 アドレスを使用して接続を試行します。 |
| 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。 |

| 電話機の IP モード | 電話機の IP アドレス | CAPF IP アドレス | 電話機から CAPF への接続方法 |
|-------------|-------------------|--------------|--|
| 2 スタック | IPv6 | IPv4、IPv6 | 電話機は、IPv6 アドレスを使用して CAPF に接続します。試行に失敗した場合、電話機は IPv4 アドレスを使用して CAPF に接続します。 |
| 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 | 電話機は、および 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 | 電話機は CAPF に接続できません。 |
| 2 スタック | IPv6 | IPv4 | 電話機は CAPF に接続できません。 |
| 2 スタック | IPv6 | IPv6 | 電話機は 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 | 電話機は、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 | 電話機は CAPF に接続できません。 |

| 電話機の IP モード | 電話機の IP アドレス | CAPF IP アドレス | 電話機から CAPF への接続方法 |
|-------------|--------------|--------------|----------------------------------|
| IPv6 スタック | IPv6 | IPv6 | 電話機は IPv6 アドレスを使用して CAPF に接続します。 |
| IPv6 スタック | IPv6 | IPv4 | 電話機は CAPF に接続できません。 |



第 7 章

セキュリティモード

- [セキュリティモードの概要 \(101 ページ\)](#)
- [非セキュアモード \(デフォルトモード\) \(101 ページ\)](#)
- [セキュアモードの設定 \(101 ページ\)](#)

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：セキュアエンドポイントと非セキュアエンドポイントをサポートします。
- SIP Auth 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)

非セキュアモードは、Unified Communications Manager を初めてインストールする場合のデフォルトのセキュリティモードです。このモードでは、Unified Communications Manager はセキュアなシグナリングや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、導入に適用するセキュリティモードを設定します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---------------|--|
| ステップ 1 | 混合モード | 混合モードを有効にして、Cisco IP 電話および Webex デバイスのセキュリティを強化します。混合モードの有効化と確認の方法について説明します。 |
| ステップ 2 | SIP OAuth モード | Cisco Jabber クライアントおよびその他デバイスのセキュリティを強化するには、SIP OAuth モードを設定します。 |

混合モード

混合モードまたはセキュアモードは、セキュアエンドポイントと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 Unified Communications Manager を新しくインストールすると、デフォルトでは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は非セキュアモードからセキュアモードまたは混合モードに変換できます。

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、次の手順を実行します。

- パブリッシャ上で認証局プロキシ機能（CAPF）サービスを有効にします。
- パブリッシャ上で証明書信頼リスト（CTL）サービスを有効にします。

Call Manager 証明書が電子署名されている場合、CTL ファイルには、サーバーごとのサーバー証明書、公開キー、シリアル番号、署名、発行者名、サブジェクト名、サーバー機能、DNS 名、および IP アドレスが含まれています。

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

電話が次回初期化されたときに、その電話ではこの CTL ファイルを TFTP サーバからダウンロードします。CTL ファイルに自己署名証明書が含まれた TFTP サーバのエントリがある場合、電話では .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、電話では署名なしの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 mixed-mode**
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 non-secure-mode**
CTL ファイルを更新し、クラスタを非セキュアモードに設定します。
- **utils ctl update CTLFile**
クラスタ内の各ノードの CTL ファイルを更新します。



- (注) エンドポイントのセキュリティのためには、シグナリングに Transport Layer Security (TLS) を使用し、メディアに Secure RTP (SRTP) を使用します。

混合モードを有効にするには、発行元ノードのコマンドラインインターフェイスにログインし、CLI コマンド `utils ctl set-cluster mixed-mode` 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信した登録トークンには、このクラスタへの登録中に [エクスポート制御機能を許可する (Allow Export-Controlled)] 機能が有効になっています。

Tokenless CTL ファイルについては、ユニファイドコミュニケーションマネージャリリース 12.0(1) で USB トークンを使用して生成されたアップロード済み CTL ファイルのダウンロードをエンドポイントで実行するよう、管理者が確認する必要があります。ダウンロード後、管理者は Tokenless CTL ファイルに切り替えることができます。次に、`utils ctl upgrade CLI` コマンドを実行することができます。

セキュリティモードを非セキュアモードからセキュアモードまたは混合モードに変更した場合は、その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の設定 (Enterprise Parameters Configuration)] ページに移動して、クラスタまたはサーバが混合モードであるかどうか確認します。詳細については、「[セキュリティモードの確認](#)」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モードからセキュアモードまたは混合モードに変更した場合は、その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の設定 (Enterprise Parameters Configuration)] ページに移動して、クラスタまたはサーバが混合モードであるかどうか確認します。

セキュリティモードを確認するには、次の手順を実行します。

- ステップ 1** [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の設定 (Enterprise Parameters Configuration)] 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 (Security Parameters)] ペインに移動します。
適切な値の [クラスタセキュリティモード (Cluster Security Mode)] フィールドがあります。値に 1 が表示されている場合、Unified Communications Manager は混合モードに正常に設定されています。Cisco Unified CM Administration ページでは、この値を設定できません。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。

CTL ファイルの SAST 役割



- (注) CTL ファイルに署名するには、次の表に記載されている*署名者が使用されます。

表 18: CTL ファイルのシステム管理者セキュリティトークン (SAST) 役割

| Cisco Unified Communications Manager のバージョン | トークンベースの CTL ファイルでの SAST 役割 | Tokenless CTL ファイルでの SAST 役割 |
|---|---|----------------------------------|
| 12.0(1) | トークン 1 (署名者*) トークン 2 ITLRecovery CallManager | ITLRecovery (署名者) CallManager |
| 11.5(x) | トークン 1 (署名者) トークン 2 ITLRecovery CallManager | CallManager (署名者) ITLRecovery |
| 10.5(2) | トークン 1 (署名者) トークン 2 | CallManager (署名者) ITLRecovery |
| 10.5(1) (サポート外) | トークン 1 (署名者) トークン 2 | CallManager (署名者) |
| 10.0(1) (サポート外) | 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 | N/A |

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登録の OAuth サポートは、Cisco Jabber デバイスおよび特定の電話機モデルで使用できます。SIP OAuth の詳細については、「[Cisco Unified Communications Manager 機能設定ガイド](#)」を参照してください。

CLI を使用した SIP OAuth 設定

CLI を使用して、クラスタ SIP OAuth モードを設定することができます。



- (注) Cisco Unified Communications Manager での SIP OAuth モードの設定方法の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*、リリース 14』を参照してください。

次の点を考慮してください。

- クラスタ SIP OAuth モードが有効になっている場合、Cisco ユニファイドコミュニケーションスマネージャーは、セキュアデバイスから OAuth トークンを受信した SIP 登録を受け入れることができます。

有効にすると、Cisco Unified Communications Manager のユーザインターフェイスを使用して設定可能な次の TLS ポートが開かれます。

- SIP OAuth ポート
- SIP OAuth MRA ポート

[Cisco Unified CM の管理 (Cisco Unified CM Administration)] から、[システム (System)] > [Cisco Unified CM] > Call Manager ページを選択します。

- パラメータ変更を反映するには、すべてのノードで Cisco CallManager サービスを再起動してください。

この暗号化方法では次の CLI コマンドを使用します。

管理者: ユーティリティ sipOAuth モード

クラスタ内の SIP OAuth モードのステータスを確認します。

ユーティリティ sipOAuth モードの有効化

クラスタ内の SIP OAuth モードを有効にします。

ユーティリティ sipOAuth モードの無効化

クラスタ内の 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。



第 8 章

SIP OAuth モード

- [SIP OAuth モードの概要 \(107 ページ\)](#)
- [SIP OAuth モードの前提条件 \(108 ページ\)](#)
- [SIP OAuth モードの設定タスク フロー \(109 ページ\)](#)

SIP OAuth モードの概要

Unified Communications Managerへのセキュア登録では、CTL ファイルの更新、共通証明書信頼ストアの設定などが行われます。デバイスが、オンプレミスとオフプレミス間で切り替わる場合、セキュア登録が完了する際は毎回、LSC と Certificate Authority Proxy Function (CAPF) 登録の更新処理が複雑になります。

SIP OAuth モードでは、セキュアな環境でのすべてのデバイスの認証に OAuth 更新トークンを使用できます。この機能により、Unified Communications Managerのセキュリティが強化されます。

Unified Communications Managerは、エンドポイントによって提示されたトークンを検証し、許可されたもののみ構成ファイルを提供します。Unified Communications Manager クラスタおよびその他のシスコのデバイスで 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。

以下で、SIP 登録の OAuth サポートが拡張されました

- Cisco Unified Communications Manager 12.5 リリース以降の Cisco Jabber デバイス
- Cisco Unified Communications Manager リリース 14 以降の SIP 電話



(注) デフォルトでは、SIP OAuth が有効になっている場合、TFTP は SIP 電話に対して安全です。TFTP ファイルのダウンロードは、認証された電話に対してのみ、セキュリティで保護されたチャネルを介して行われます。SIP OAuth は、オンプレミスおよび MRA を介して CAPF を使用せずに、エンドツーエンドの安全なシグナリングとメディア暗号化を提供します。

次に、OAuth 用に設定できる電話セキュリティプロファイルのタイプを示します。

- Cisco Dual Mode for iPhone (TCT デバイス)
- Cisco Dual Mode For Android (BOT デバイス)
- Cisco Unified Client Services Framework (CSF デバイス)
- Cisco Jabber for Tablet (TAB デバイス)
- ユニバーサル デバイス テンプレート (Universal Device Template)
- Cisco 8811
- Cisco 8841
- Cisco 8851
- Cisco 8851NR
- Cisco 8861
- Cisco 7811
- Cisco 7821
- Cisco 7841
- Cisco 7861
- Cisco 8845
- Cisco 8865
- Cisco 8865NR
- Cisco 7832
- Cisco 8832
- Cisco 8832NR

SIP OAuth モードの前提条件

この機能は、次の作業が完了していることを前提としています。

- モバイルおよびリモートアクセスが設定されていること、および接続がユニファイドコミュニケーションマネージャとエクスプレス Sway の間で確立されていることを確認します。
- [エクスポート制御機能を許可する (**allow export-controlled**)] 機能を使用して Unified Communications Manager が Smart または Virtual アカウントに登録されていることを確認します。
- クライアントファームウェアが SIPOAuth をサポートしていることを確認します。

SIP OAuth モードの設定タスク フロー

システムの SIP OAuth を設定するには、次のタスクを実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | Phone Edge Trust へのCA証明書のアップロード | トークンを取得するには、CA 証明書を電話エッジトラストにアップロードします。この手順は、Cisco Jabber デバイスには適用されません。 |
| ステップ 2 | デバイスの OAuth アクセストークンを有効にする | 重要 この手順は、リリース 14 以降に適用されます。 Cisco IP電話 7800 および 8800 エンタープライズシリーズの SIP 登録で OAuth を有効にします。この手順は、Cisco Jabber デバイスには適用されません。 |
| ステップ 3 | 更新ログインの設定 (111 ページ) | SIP OAuth を介してデバイスを登録するために、Unified Communications Manager で更新ログインフローを使用した OAuth を有効化する。 |
| ステップ 4 | OAuth ポートの設定 (111 ページ) | OAuth が登録されているノードごとに、OAuth 用のポートを割り当てます。 |
| ステップ 5 | OAuth Connection を Expressway-C に設定 (112 ページ) | 相互認証された TLS 接続をデュアルに設定します -C。 |
| ステップ 6 | SIP OAuth モードの有効化 (113 ページ) | パブリッシャ ノードで CLI コマンドを使用して OAuth サービスを有効にします。 |
| ステップ 7 | Cisco CallManager サービスの再起動 (113 ページ) | OAuth が登録されているすべてのノードで、このサービスを再起動します。 |
| ステップ 8 | 電話セキュリティプロファイルでデバイスセキュリティモードを設定する | エンドポイントに対して暗号化を展開する場合、電話セキュリティプロファイルで、OAuth サポートを設定します。 |
| ステップ 9 | (任意) SIPOAuth 登録済み電話を MRA モード用に構成する | 重要 この手順は、リリース 14 以降に適用されます。 SIPOAuth 登録済みの電話を MRA モードで構成します。この手順は、Cisco Jabber デバイスには適用されません。 |

Phone Edge TrustへのCA証明書のアップロード

この手順を使用して、Tomcat 署名付き証明書のルート証明書を Phone EdgeTrust にアップロードします。



(注) この手順は Cisco Phone に対してのみ実行され、Cisco Jabber には適用されません。

- 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 [Upload Certificate/Certificate chain] 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] ウィンドウで、[証明書の目的] ドロップダウンリストから [電話-エッジ-信頼] を選択します。
- ステップ 4 [ファイルのアップロード] フィールドで、[参照] をクリックして証明書をアップロードします。
- ステップ 5 [アップロード (Upload)] をクリックします。

デバイスの OAuth アクセストークンを有効にする



重要 このセクションは、リリース 14 以降に適用されます。

この手順を使用して、電話の OAuth アクセストークンを有効にします。



(注) このエンタープライズパラメータは、電話の SIP 登録の OAuth サポートに対してのみ設定してください。

- ステップ 1 Cisco Unified CM Administration から、[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。
- ステップ 2 [SSOとOAuthの構成] セクションで、[デバイスのOAuthアクセストークン] ドロップダウンリストの値が [暗黙的：既に登録されているデバイス] に設定されていることを確認します。
- (注) デバイスの OAuth アクセストークンの値を **Explicit:Activation Code** に設定します。デバイスのオンボーディングは、SIPOAuth 登録のトークンの暗黙的な受信を無効にし、アクティベーションコードを介したトークンの受信のみをサポートするために必要です。セキュリティプロファイルに示されている場合、トークンは SIPOAuth 登録に使用できます。
- リリース 14 以降、デバイスのエンタープライズパラメータ **OAuth アクセストークン** のデフォルト値は **Implicit : Alreadyregistereddevices** です。

ステップ3 [保存 (Save)] をクリックします。

更新ログインの設定

OAuth アクセストークンを使用して更新ログインを設定し、Cisco Jabber クライアントのトークンを更新するには、次の手順を使用します。

- ステップ1 Cisco Unified CM の管理から、[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。
- ステップ2 [SSO および OAuth 構成 (SSO and OAuth Configuration)] で、**OAuth with Refresh Login Flow** のパラメータを [有効 (Enabled)] にします。
- ステップ3 (任意) [SSO および OAuth の設定 (SSO And OAuth Configuration)] セクションで、その他のパラメータを設定します。パラメータの説明を確認するには、パラメータ名をクリックします。
- ステップ4 [保存 (Save)] をクリックします。

OAuth ポートの設定

SIP OAuth に使用するポートを割り当てるには、次の手順を使用します。

- ステップ1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。、[システム (System)] > [Cisco Unified CM]。
- ステップ2 SIP OAuth を使用するサーバごとに次の操作を行います。
- ステップ3 サーバを選択します。
- ステップ4 [Cisco Unified Communications Manager (Cisco Unified Communications Manager)] の [TCP ポートの設定 (TCP Port Settings)] で、次のフィールドに対してポート値を設定します。
 - SIP 電話 OAuth ポート (SIP Phone OAuth Port)
デフォルト値は5090です。設定可能な範囲は 1024 ~ 49151 です。
 - SIP モバイルおよびリモートアクセス ポート (SIP Mobile and Remote Access Port)
デフォルト値は5091です。設定可能な範囲は 1024 ~ 49151 です。

(注) Cisco Unified Communications Manager は、SIP Phone OAuth Port (5090) を使用して、TLS 経由の Jabber OnPremise デバイスから SIP 回線登録をリッスンします。ただし、ユニファイド CM は、SIP モバイルリモートアクセスポート (デフォルトは 5091) を使用して、mTLS を介して Jabber からの SIP 回線登録をリッスンします。

両方のポートは、着信 TLS/mTLS 接続に Cisco Tomcat 証明書と Tomcat 信頼を使用します。Tomcat 信頼ストアがモバイルおよびリモートアクセスの SIP OAuth モード用の Mra C 証明書を正確に機能させることを確認できることを確認します。

次の場合に、Cisco Unified Communications Manager の Tomcat 信頼証明書ストアに Expressway-C 証明書をアップロードするための追加の手順を実行する必要があります。

- Expressway-C 証明書と Cisco Tomcat 証明書は、同じ CA 証明書によって署名されていません。
- Unified CM Cisco Tomcat 証明書は CA 署名されていません。

ステップ 5 [保存 (Save)] をクリックします。

ステップ 6 SIP OAuth を使用する各サーバに対して、この手順を繰り返します。

OAuth Connection を Expressway-C に設定

Cisco Unified Communications Manager Administration に Expressway-C 接続を追加するには、次の手順を使用します。SIP OAuth を使用するモバイルおよびリモートアクセス モードのデバイスには、この構成が必要です。

ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。デバイス > Expressway-C

ステップ 2 (任意) [Expressway-C の検索とリスト] ウィンドウで、[検索] をクリックして、Expressway-C から Unified Communications Manager にプッシュされた X.509 サブジェクト名/サブジェクト代替名を確認します。

(注) 必要に応じて値を変更できます。また、エントリが存在しない場合は、Expressway-C 情報を追加します。

ユニファイドコミュニケーションマネージャとは別のドメインを持っている場合、管理者は Cisco Unified CM の管理ユーザインターフェイスにアクセスして、Unified CM の設定でドメインを Expressway-C に追加する必要があります。

ステップ 3 [新規追加] をクリックします。

ステップ 4 Expressway-C に対して、IP アドレス、ホスト名または、完全修飾ドメイン名を入力します。

ステップ 5 Description を入力します。

ステップ 6 X.509 のサブジェクト名/サブジェクトの代替名を、入力 Sway-C 証明書から入力します。

ステップ 7 [保存 (Save)] をクリックします。

SIP OAuth モードの有効化

SIPOAuthモードを有効にするには、コマンドラインインターフェイスを使用します。パブリッシャノードでこの機能を有効にすると、すべてのクラスタノードの機能もイネーブルになります。

Before you begin

リリース 14SU1 以降、プロキシ TFTP が有効になっている場合は、クラスタ外 Tomcat 証明書のルート CA 証明書をプロキシ電話エッジ信頼にコピーする必要があります。

-
- ステップ 1** Unified Communications Manager のパブリッシャ 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** `utils sipOAuth-mode enable` の CLI コマンドを実行します。
リリース 14SU1 以降、システムは、読み取り専用のクラスタ **SIPOAuth** モードエンタープライズパラメータを有効に更新します。
-

Cisco CallManager サービスの再起動

CLI で SIP OAuth を有効にした後に、SIP OAuth を介してエンドポイントが登録されるすべてのノードで Cisco CallManager サービスを再起動します。

-
- ステップ 1** [Cisco Unified Serviceability] から選択します。[ツール (Tools)] > [コントロールセンター (ControlCenter)] > [機能サービス (Feature Services)]。
- 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。
- ステップ 3** Cisco CallManager サービスを確認し、[再起動 (Restart)] をクリックします。
-

電話セキュリティプロファイルでデバイスセキュリティモードを設定する

この手順を使用して、電話機のセキュリティプロファイルでデバイスセキュリティモード (**Device Security Mode**) を設定します。これは、その電話機の[電話機のセキュリティプロファイル (Phone Security Profile)]内でデバイスセキュリティモードを[暗号化 (Encrypted)]に設定している場合にのみ必要です。

-
- ステップ 1** [Cisco Unified CM の管理 (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** 次のいずれかを実行します。
- 既存の電話セキュリティプロファイルを検索する

- [新規追加 (Add New)] をクリックします。

ステップ 3 [電話セキュリティプロファイル情報 (Phone Security Profile Information)] セクションの [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、[暗号化 (Encrypted)] を選択します。

ステップ 4 [転送タイプ (Transport type)] ドロップダウンリストで、[TLS] を選択します。

ステップ 5 [OAuth 認証の有効化 (Enable OAuth Authentication)] チェックボックスをオンにします。

ステップ 6 [保存 (Save)] をクリックします。

ステップ 7 電話セキュリティプロファイルを電話に関連付けます。電話セキュリティ電話を適用する方法の詳細については、[Cisco Unified Communications Manager セキュリティ ガイド](#)の「セキュリティプロファイルを電話に適用する」セクションを参照してください。

(注) 変更を有効にするには、スマートフォンをリセットしてください。

(注) [SIP OAuth モード (SIP OAuth Mode)] が有効な場合、[ダイジェスト認証を有効化 (Enable Digest Authentication)] および [TFTP 暗号化設定 (TFTP Encrypted Config)] オプションはサポートされません。電話機は、[https\(6971\)](https://6971)を介して TFTP 設定ファイルを安全にダウンロードし、認証にトークンを使用します。

SIPOAuth 登録済み電話を MRA モード用に構成する

この手順を使用して、SIPOAuth 登録済み電話を MRA モードに構成します。

Before you begin



Important このセクションは、リリース 14 以降に適用されます。

電話機がアクティベーションコードを使用するように設定されていることを確認してください。詳細については、[Cisco Unified Communications Manager システム設定ガイド](#)の「アクティベーションコードを使用するための登録方法の設定」セクションを参照してください。



Note SIP OAuth over MRA を使用する場合、ユーザーはログインにユーザー名/パスワードを使用できませんが、オンボーディングに基づくアクティベーションコードを使用する必要があります

ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[デバイス (Device)] > [電話 (Phone)]。

ステップ 2 [検索] をクリックして、オフプレミスモード用に構成するデバイスを選択します。

ステップ 3 [デバイス情報] セクションで、次の手順を実行します。

- **[MRA経由でアクティベーションコードを許可する (Allow Activation Code via MRA)]** チェックボックスをオンにします。
- **[アクティベーションコードMRAサービスドメイン]** ドロップダウンリストから、必要な MRA サービスドメインを選択します。MRA サービスドメインを設定する方法の詳細については、[Cisco Unified Communications Manager システム設定ガイド](#)の「*MRA* サービスドメインの設定」セクションを参照してください。

Note SIP OAuth over MRA モードの場合、アクティベーションコードのみを使用し、ユーザー名/パスワードベースのログインは使用しないでください。

ステップ 4 **[プロトコル固有の情報]** セクションで、**[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 OAuth 対応の SIP プロファイルを選択します。電話機が OAuth ファームウェアをサポートしていることを確認してください。セキュリティプロファイルの作成方法の詳細については、[Cisco Unified Communications Manager システム設定ガイド](#)の「電話セキュリティプロファイルの設定」セクションを参照してください。

ステップ 5 **[保存 (Save)]** と **[構成の適用 (Apply Configuration)]** をクリックします。

Note 電話機は MRA モードに切り替わり、Expressway との通信を開始します。内部ネットワークでオンプレミスからのライン Sway との通信が許可されていない場合、電話機は登録されませんが、オフプレミスの電源がオンになっているときには、その電話機に接続する準備ができています。



第 9 章

TFTP 暗号化

- [暗号化された TFTP 設定ファイルの概要 \(117 ページ\)](#)
- [電話機の設定ファイルの暗号化のタスクフロー \(119 ページ\)](#)
- [暗号化された TFTP 設定ファイルの無効化 \(123 ページ\)](#)

暗号化された TFTP 設定ファイルの概要

TFTP 設定は、電話機が登録プロセスを実行する際に 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って、デバイスの登録プロセス中に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、電話機の SSH ログイン情報などの機密情報が含まれます。この機能が設定されていない場合、設定ファイルはクリアテキストで送信されます。この機能を導入すると、登録プロセス中に攻撃者がこの情報を傍受できなくなります。この情報は暗号化解除され、クリアテキストで送信されます。したがって、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 電話でダイジェスト認証オプションを有効にし、TFTP で暗号化設定オプションを無効にした場合は、ダイジェストログイン情報がクリアテキストで送信されます。

TFTP の設定後、TFTP サーバは次の手順を実行します。

- ディスク上のクリアテキストの設定ファイルをすべて削除します
- 暗号化されたバージョンのコンフィギュレーションファイルを生成します。

電話機が暗号化された電話設定ファイルをサポートし、電話設定ファイルの暗号化に必要なタスクを行った場合は、電話機は設定ファイルの暗号化バージョンを要求します。

一部の電話は、暗号化された電話設定ファイルをサポートしません。電話機のモデルとプロトコルによって、コンフィギュレーションファイルを暗号化するためにシステムが使用する方法が決定されます。サポートされる方式は、Unified Communications Manager の機能と、暗号化された設定ファイルをサポートするファームウェアロードに依存します。電話のファームウェアロードを、暗号化に対応していないバージョンにまでダウングレードすると、TFTP サーバは

最低限の設定を行う暗号化されていない設定ファイルを送ります。この場合、電話が期待された機能を発揮できないことがあります。

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できるように、暗号化された電話設定ファイルに関連するタスクをセキュアな環境で実行することを推奨します。

Unified Communications Manager は、次の方式をサポートします。

- 手動キー配布
- 電話の公開キーによる対称キーの暗号化

手動キー配布と電話の公開キーによる対称キー暗号化のための設定情報は、混合モードが設定済みで、[Unified Communications Manager Administration] の [TFTP 暗号化設定 (TFTP Encrypted Config)] パラメータが有効になっていることを前提としています。

暗号化された TFTP 設定ファイルのヒント

電話機のダウンロードで機密データを保護するには、TFTP 暗号化設定ファイルを有効にすることをお勧めします。電話に PKI 機能がない場合、[Unified Communications Manager Administration] と電話で対称キーも設定する必要があります。対称キーが電話機または Unified Communications Manager のいずれかに存在しない場合、または TFTP 暗号化設定ファイルの設定時に不一致が発生した場合、電話機は登録できません。

Unified Communications Manager で暗号化された設定ファイルを設定する場合は、次の点を考慮してください。

- 暗号化された設定ファイルをサポートしている電話機にのみ、[電話機のセキュリティプロファイルの設定 (Phone Security Profile Configuration)] ページに [TFTP 暗号化設定 (TFTP Encrypted Config)] チェックボックスが表示されます。暗号化された設定ファイルを Cisco Unified IP Phone の 7800、7942、および 7962 (SCCP のみ) に設定することはできません。これらの電話機は設定ファイルのダウンロードで機密データを受信しないからです。
- デフォルトでは、[TFTP 暗号化設定 (TFTP Encrypted Config)] チェックボックスはオフになっています。このデフォルト設定、非セキュアプロファイルを電話機に適用した場合、ダイジェストログイン情報とセキュアパスワードはクリアテキストで送信されます。
- 公開キー暗号化を使用する Cisco Unified IP Phone の場合、Unified Communications Manager では [デバイスセキュリティモード (Device Security Mod)] を [認証済み (Authenticated)] または [暗号化 (Encrypted)] に設定して暗号化された設定ファイルを有効にする必要はありません。Unified Communications Manager は、登録中の公開鍵をダウンロードするために CAPF プロセスを使用します。
- 環境が安全である場合や、PKI が有効になっていない電話機に対称キーを手動で設定しないようにする場合は、暗号化されていない設定ファイルを電話機にダウンロードできます。ただし、この方法を使用することはお勧めしません。

- Cisco Unified IP Phone の 7800、7942、および 7962（SIP のみ）では、Unified Communications Manager は暗号化された設定ファイルを使用するよりも簡単で、安全性が低いダイジェストログイン情報を電話機に送信する方法を提供します。[ダイジェストログイン設定ファイルを除外（Exclude Digest Credentials in Configuration File）]設定を使用するこの方法は、最初に対称キーを設定して電話に入力する必要がないため、ダイジェストログイン情報の初期化に役立ちます。この方法では、暗号化されていないコンフィギュレーションファイルで、電話機にダイジェストクレデンシャルを送信します。ログイン情報が電話機に入力された後は、[TFTP 暗号化設定（TFTP Encrypted Config）] オプションを無効にしてから、[電話機のセキュリティプロファイルの設定（Phone Security Profile Configuration）] ページの [設定ファイルのダイジェストクレデンシャルを除外する（Exclude Digest Credential in Configuration File）] 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ログイン情報が除外されます。
- ダイジェストログイン情報が電話に存在するようになり、着信ファイルにダイジェストログイン情報が含まれないとなると、既存のログイン情報がそのまま使用されます。ダイジェストクレデンシャルは、電話機が工場出荷時の状態にリセットされるか、または新しいクレデンシャル(空白を含む)を受信するまで、そのまま残ります。電話機またはエンドユーザのダイジェストログイン情報を変更する場合は、対応する[電話機のセキュリティプロファイル情報（Phone Security Profile Information）] ページの [設定ファイルでのダイジェストログイン情報の除外（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ログイン情報を電話機にダウンロードします。

電話機の設定ファイルの暗号化のタスクフロー

TFTP 設定ファイルの暗号化を設定するには、クラスタのセキュリティが混合モードで設定されていることを確認し、手動キー暗号化と公開キー暗号化をサポートするクラスタ内の電話機を確認し、SHA-1 と SHA-512 をサポートする電話機を確認し、以下のタスクを完了します。



(注) SHA-512 クラスタ全体を有効にし、電話機がサポートしていない場合、これらの電話機は機能しません。

手順

| | コマンドまたはアクション | 目的 |
|--------|-------------------------------|--|
| ステップ 1 | TFTP 暗号化の有効化 (120 ページ) | 電話機の [TFTP 設定ファイル (TFTP Configuration File)] 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することができます。 |
| ステップ 2 | SHA-512 署名アルゴリズムの設定 (120 ページ) | TFTP ファイル暗号化を有効化すると、デフォルトの署名アルゴリズムとして SHA-1 が設定されます。 |

| | コマンドまたはアクション | 目的 |
|--------|-------------------------------------|---|
| | | より強力な SHA-512 アルゴリズムを使用するようにシステムを更新するには、次の手順を使用します。 |
| ステップ 3 | LSC または MIC 証明書のインストールの確認 (121 ページ) | 公開キーを使用する電話機の場合は、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 (122 ページ) | TFTP 設定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 (122 ページ) | Cisco CallManager サービスおよび Cisco TFTP サービスを再起動します。 |
| ステップ 6 | 電話のリセット (122 ページ) | 暗号化された TFTP 設定ファイルの更新が完了したら、電話機をリセットします。 |

TFTP 暗号化の有効化

この TFTP は、特定のモデルの電話の電話セキュリティプロファイル内で有効にできます。TFTP サーバからダウンロードするファイルの TFTP 暗号化を有効にするには、次の手順を実行します。

-
- ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[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)]
- ステップ 2 [検索 (Find)] 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 Encrypted Config] 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。
- ステップ 5 クラスタで使用されている他のすべて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) 電話設定ファイルの暗号化を無効にするには、Cisco Unified Communications Manager Administration の電話セキュリティプロファイルで [TFTP 暗号化設定 (TFTP Encrypted Config)] チェックボックスをオフにして、変更内容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 ファイル暗号化のデフォルトのアルゴリズムです。次のオプションの手順を使用して、デジタル署名などの TFTP 設定ファイルにより強力な SHA-512 アルゴリズムを使用するようにシステムをアップグレードできます。



- (注) ご使用の電話機が SHA-512 をサポートしていることを確認してください。対応していない場合は、システム更新後に電話機が動作しなくなります。

ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[システム (System)] > [エンタープライズパラメータ (Enterprise Parameters)]

ステップ 2 [セキュリティパラメータ (Security Parameters)] ペインに移動します。

ステップ 3 [TFTP File Signature Algorithm] 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。

この手順を完了するには、ポップアップウィンドウに一覧表示されている影響を受けるサービスを再起動します。

LSC または MIC 証明書のインストールの確認

公開キーを使用する電話機の場合は、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 Phone に適用されます。電話機が PKI 暗号化をサポートしているかどうかを確認するには、「暗号化された設定ファイルをサポートする電話モデル」の項を参照して

次の手順は、電話機が Unified Communications Manager データベースに存在し、Unified Communications Manager で [TFTP 暗号化設定 (TFTP Encrypted Config)] パラメータを有効にしていることを前提としています。

ステップ 1 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 (Device)] > [電話機 (Phone)] の順に選択します。電話機のリストが表示されます。

ステップ 3 [デバイス名 (Device Name)] をクリックします。
[電話の設定 (Phone Configuration)] ページが表示されます。

ヒント [電話の設定 (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て、Unified Communications Manager の電話機に LSC または MIC が存在するかどうかを確認します。証明書が電話機に存在しない場合、[削除 (Delete)] および [トラブルシューティング (Troubleshoot)] オプションは表示されません。

ヒント 電話機のセキュリティ設定を確認することによって、電話機に LSC または MIC が存在することを確認することもできます。詳細については、Unified Communications Manager のこのバージョンをサポートする Cisco Unified IP Phone の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 4 証明書が存在しない場合、[電話の設定 (Phone Configuration)] ウィンドウで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。LSC のインストール方法については、Certificate Authority Proxy Function に関連するトピックを参照してください。

ステップ 5 CAPF を設定したら、[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、TFTP サーバから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 の変更を行った後、CTL ファイルを更新します。TFTP ファイル暗号化を有効にしているため、CTL ファイルを再生成する必要があります。

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 パブリッシュャ 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

暗号化された TFTP 設定ファイルの更新を完了したら、Cisco TFTP サービスと Cisco CallManager サービスを再起動して変更を有効にしてください。

ステップ 1 [Cisco Unified Serviceability] から選択します。[ツール (Tools)] > [コントロールセンター - 機能サービス (Control Center - Feature Services)]

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。ただし、CallManager 証明書を再生成または更新した後は、TFTP サービスを手動で再起動する必要はありません。

電話のリセット

すべての暗号化された TFTP 設定ファイルの更新が完了したら、電話機をリセットしてください。

ステップ 1 [Cisco Unified CM Administration] から、[デバイス (Device)] > [電話 (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 (Select All)] をクリックします。

ステップ 4 [選択をリセットする (Reset selected)] をクリックします。

暗号化された TFTP 設定ファイルの無効化



警告 TFTP 暗号化設定が **[False]** であるが、SIP を実行している電話でダイジェスト認証が **[True]** に設定されている場合、ダイジェストログイン情報がクリアテキストで送信される可能性があります。

設定を更新した後、電話機の暗号キーは Unified Communications Manager データベースに残ります。

Cisco Unified IP Phone 7911G、7931G (SCCP のみ)、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7971G および 7975G は暗号化ファイル (.enc、.sgn ファイル) を要求します。暗号化設定が **False** に更新された場合は、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) を要求します。

Cisco Unified IP Phone は、SCCP および SIP 上で実行されている場合に、暗号化設定が **False** に更新されると、暗号化されたファイルを要求します。次回リセットされたときに電話が暗号化されていない設定ファイルを要求するように設定するには、電話の GUI から対称キーを削除します。

- Cisco Unified IP Phone SCCP で実行される Cisco Unified IP 電話は、6901、6911、6921、6941、6945、6961、7906G、7911G、7921G、7925G、7925G-EX、7926G、7931G、7940G、7941G、7941G-GE、7942G、7945G、7960G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、7975G、8941、8945 です。
- Cisco Unified IP Phone SIP で実行される Cisco Unified IP 電話は、6901、6911、6921、6941、6945、6961、7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G、7962G、7965G、7970G、7971G、7971G-GE、7975G、8941、8945、8961、9971、7811、78321、7841、7861、7832、8811、8841、8845、8851、8851NR、8861、8865、8865NE、8821、8831、8832、8832NR です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|----|
| ステップ 1 | 電話機設定ファイルの暗号化を無効にするには、電話機に関連付けられている電話機のセキュリティ | |

暗号化された TFTP 設定ファイルの無効化

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | ロファイルの [TFTP 暗号化設定 (TFTP Encrypted Config)] チェックボックスをオフにします。 | |
| ステップ 2 | Cisco Unified IP Phone 7942 および 7962 (SIP のみ) の場合は、電話画面で対称キーのキー値として「32-byte 0」を入力して暗号化を無効にします。 | |
| ステップ 3 | Cisco Unified IP Phone (SIP のみ) の場合は、電話画面で対称キーを削除して暗号化を無効にします。 | これらの作業の実行方法については、使用している電話のモデルに対応する電話のアドミニストレーションガイドを参照してください。 |



第 10 章

暗号管理

- [暗号管理 \(125 ページ\)](#)
- [暗号ストリングの設定 \(128 ページ\)](#)
- [暗号の制限 \(131 ページ\)](#)
- [暗号の制限 \(144 ページ\)](#)

暗号管理

暗号の管理はオプションの機能で、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制御できます。暗号管理を使用すると、弱い暗号を無効にして最小レベルのセキュリティを有効にすることができます。

[**Cipher Management**] ページには、デフォルト値はありません。代わりに、暗号化管理機能は、許可されている暗号を設定している場合にのみ有効になります。[**暗号管理 (Cipher Management)**] ページで設定している場合でも、特定の弱い暗号は許可されません。

次の TLS インターフェイスおよび SSH インターフェイスで暗号を設定することができます。

- [**All TLS (すべての TLS)**] : このフィールドに割り当てられている暗号は、Unified Communications Manager および IM and Presence Service の TLS プロトコルをサポートするすべてのサーバおよびクライアント接続に適用されます。
- [**HTTPS TLS**] : このフィールドに割り当てられる暗号は、Unified Communications Manager および IM and Presence Service の TLS プロトコルをサポートするポート 443 および 8443 上のすべての 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割り当てる場合、[**HTTPS TLS**] 上で設定されている暗号が [**すべての TLS (All TLS)**] 暗号を上書きします。

- **SIP TLS**: このフィールドに割り当てられる暗号は、ユニファイドコミュニケーションマネージャー上の TLS プロトコルをサポートする sip tls インターフェイスを介して送受信さ

れる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。

認証モードの SIP インターフェイスは、ナル-SHA 暗号のみをサポートしています。

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化を設定した場合は、認証モードはサポートされなくなります。

SIP TLS および **ALL TLS** フィールドで暗号を割り当てる場合、SIP TLS で設定した暗号は、ALL TLSs 暗号を上書きします。

- [SSH 暗号 (SSH Ciphers)] : このフィールドに割り当てられる暗号は、Unified Communications Manager および IM and Presence Service の SSH 接続に適用されます。
- [SSH キー交換 (SSH Key Exchange)] : このフィールドで割り当てられるキー交換アルゴリズムは、Unified Communications Manager および IM and Presence Service の SSH インターフェイスに適用されます。

カーブのネゴシエーション

次に、曲線のネゴシエーションの点を示します。

- ECDSA の暗号は、ECDSA 証明書のキーサイズに基づいて、さまざまな EC カーブとネゴシエートされます。
- RSA の暗号化は、証明書のキーサイズに関係なく、すべての EC カーブとネゴシエートされます。
- ECDSA 証明書のキーサイズは、TLS ネゴシエーションを発生させるための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 のカーブを提供する場合、384 キー証明書と ECDSA の暗号がネゴシエートされます。

曲線のネゴシエーションは、RSA 暗号と ECDSA 暗号の両方のクライアント設定に基づいています。

証明書のサイズが 384 ビットであり、クライアントのオファーリングが P-521 の場合、P-384 P-256 EC のネゴシエーションが発生すると、P-521 の曲線で TLS ネゴシエーションが発生します。クライアントによって提供されるカーブは最初の P-521 であり、P-384 曲線もリストから利用できます。証明書サイズが 384 ビットであり、クライアントオファーリングが P-521、P-256 の場合、P-384 曲線がクライアントによって提供されないため、TLS ネゴシエーションは行われません。

EC カーブでサポートされている暗号を次に示します。

```
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 および IM and Presence Service は、サードパーティ製品を含む他のほとんどの製品との安全な統合をサポートする一連の暗号（下記の TLS および SSH 暗号のセクションを参照）をすでに使用しています。したがって、通常は変更を加え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は、Unified Communications Manager 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暗号を追加できます。

暗号管理は、顧客がより制限を加えて、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ないようにしたい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 SSHMAC インターフェイスで sha2-512 を設定すると、DRS と CDR の機能が影響を受けます。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 key " 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。

シスコでは、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
```

暗号ストリングの設定

- [すべての TLS (All TLS)]、[SIP TLS]、および [HTTPS TLS] フィールドに必ず暗号ストリングを OpenSSL 暗号ストリング形式で入力してください。
- また、[SSH 暗号 (SSH Ciphers)]、[SSH MAC] のアルゴリズム、および [SSH キー交換 (SSH Key Exchange)] フィールドには、OpenSSH 形式で暗号またはアルゴリズムも入力してください。
- 「推奨される暗号 (127 ページ) 」を確認してください。

異なるセキュアなインターフェイスで暗号ストリングを設定するには、「暗号の制限事項」セクションを参照してください。

ステップ 1 [Cisco Unified OS の管理 (Cisco Unified OS Administration)] から、[セキュリティ (Security)] > [暗号の管理 (Cipher Management)] を選択します。

[暗号の管理 (Cipher Management)] ページが表示されます。

ステップ 2 ALL TLS、SIP TLS、HTTPS TLS フィールドで暗号ストリングを設定するには、暗号ストリングを OpenSSL 暗号ストリングフォーマットで [暗号ストリング (Cipher String)] フィールドに入力します。

ステップ 3 次のフィールドに暗号ストリングを設定しない場合に発生する状況を以下に示します。

- [すべての TLS (All TLS)] または [HTTPS TLS] フィールド : HTTPS TLS インターフェイスポート (8443) は、[エンタープライズパラメータ (Enterprise parameters)] (HTTPS 暗号) ページから設定を実行します。
- [すべての TLS (All TLS)] または [SIP TLS] フィールド : SIP インターフェイスポート (5061) は、暗号化モードの [エンタープライズパラメータ] (TLS 暗号) ページと認証モードの NULL-SHA 暗号から設定を取得します。

(注) [HTTPS TLS] または [SIP TLS] フィールドに暗号ストリングを設定しない場合、システムはデフォルトで [ALL TLS (すべての TLS)] フィールドから設定を取得します。

OpenSSL 暗号ストリングの形式の詳細については、<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 暗号化、フィールドで暗号ストリングを設定するには、暗号ストリングを OpenSSL 暗号ストリングフォーマットで [暗号ストリング (Cipher String)] フィールドに入力します。

SSH 暗号の OpenSSH 暗号ストリング形式の詳細については、https://www.ssh.com/manuals/server-admin/44/Ciphers_and_MACs.html を参照してください。

[SSH 暗号 (SSH Ciphers)] フィールドに暗号文字列を設定しなかった場合、デフォルトでは、次の暗号がすべての SSH 接続に適用されます。

FIPS モードで、次のようになります。

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

非 FIPS モードで、次のようになります。

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

ステップ 5 [SSH キー交換 (SSH Key Exchange)] のキー交換アルゴリズムを設定するには、**[アルゴリズム文字列 (Algorithm String)]** フィールドにアルゴリズム文字列を OpenSSH 文字列形式で入力します。

SSH キー交換用の OpenSSH アルゴリズム文字列形式の詳細については、<https://tools.ietf.org/id/draft-ietf-curdle-ssh-kex-sha2-09.html> を参照してください。

[SSH キー交換 (SSH Key Exchange)] フィールドでキー交換アルゴリズムを設定しなかった場合、デフォルトでは、次のキー交換アルゴリズムがすべての SSH 接続に適用されます。

FIPS モードで、次のようになります。

```
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 モードで、次のようになります。

```
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 [SSH MAC] フィールドで MAC アルゴリズムを設定するには、**[アルゴリズム文字列 (Algorithm String)]** フィールドにアルゴリズム文字列を OpenSSH 文字列形式で入力します。

SSH MAC の OpenSSH アルゴリズム文字列形式の詳細については、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かった場合、次の MAC アルゴリズムがデフォルトですべての SSH 接続に適用されます。

FIPS モードで、次のようになります。

```
hmac-sha1
```

非 FIPS モードで、次のようになります。

```
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 (Cipher Expansion String)]** および **[アルゴリズム拡張文字列 (Algorithm Expansion String)]** 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**、**STP TLS**、**HTTPS TLS**、および**SSH 暗号化**における暗号化を検証し、**[実際の暗号方式 (Actual Ciphers)]** フィールドに自動的に暗号方式を入力します。

[暗号ストリング (Cipher String)] フィールドに無効な暗号が入力されると、**[暗号化拡張文字列 (Cipher Expansion String)]** フィールドに自動的な入力が行われず、以下のエラーメッセージが表示されます。

無効な暗号ストリングが入力されました

システムは、**[SSHキー交換 (SSH Key Exchange)]** 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 (Algorithm Expansion String)]** フィールドに自動的にアルゴリズム文字列を入力します。

[アルゴリズム文字列 (Algorithm String)] フィールドに無効なアルゴリズムが入力されると、**[アルゴリズム拡張文字列 (Algorithm Expansion String)]** フィールドに自動的な入力が行われず、以下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が入力されました

- (注) **[実際の暗号方式 (Actual Ciphers)]** または **[実際のアルゴリズム (Actual Algorithms)]** フィールドに自動的に入力される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す。システムは、**[暗号拡張文字列 (Cipher Expansion String)]** または **[アルゴリズム拡張文字列 (Algorithm Expansion String)]** 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に暗号を設定した場合は、それぞれのサービスをリブートまたは再起動する必要があります。

表 19: 設定された暗号と対応するアクション

| 設定された暗号フィールド | 操作 |
|-----------------------------|---|
| All TLS | 暗号ストリングを有効にするために、クラスタ内のすべてのノードをリブートします。 |
| HTTPS TLS | 暗号ストリングを有効にするため、すべてのノードで Cisco Tomcat サービスを再起動します。 |
| SIP TLS | 暗号ストリングを有効にするために、すべてのノードで Unified Communications Manager を再起動します。 |
| SSH 暗号 | 暗号ストリングを有効にするために、クラスタ内のすべてのノードをリブートします。 |
| SSH キー交換 または SSH MAC | アルゴリズム文字列を有効にするために、クラスタ内のすべてのノードをリブートします。 |



- (注) 暗号は、[暗号の管理 (Cipher Management)] ページの [暗号ストリング (Cipher String)] フィールドに入力して有効にできます。これらの暗号を入力しない場合は、アプリケーションでサポートされているデフォルトの暗号すべてが有効になります。ただし、[暗号の管理 (Cipher Management)] ページの [暗号ストリング (Cipher String)] フィールドに暗号ストリングを入力しない場合は、特定の弱い暗号を無効にすることもできます。

暗号の制限

[Cipher Management configuration] 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。たとえば、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」セクションを参照してください。



- (注) [暗号管理 (Cipher Management)] ページで暗号が構成されているクラスターをアップグレードする場合は、[すべて (ALL)] フィールドと [HTTPS] フィールドの間に少なくとも 1 つの共通暗号を構成するようにしてください。

GUI での検証

[暗号管理 (Cipher Management)] 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、次のように設定されている暗号があるとします。失敗しました。!MD5、暗号文字列は "不良" は暗号化されていないことを認識していても、有効であると見なされません。OpenSSL は、これを有効な文字列と見なします。AES128-SHA ではなく、AES128_SHA が設定されている場合 (ハイフンの代わりに下線を使用)、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** : [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 (Device Security Profile)] が [認証済み (Authenticated)] 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。

[エンタープライズパラメータ (Enterprise Parameter)] 「[TLS の暗号 (TLS Ciphers)]」が、「[サポートされているすべての暗号 (ALL Supported Ciphers)]」を使用して設定されていて、[暗号管理 (Cipher Management)] ページが、[すべての TLS (All TLS)] インターフェイスの「AES256-GCM-SHA384:AES256-SHA256」暗号によって設定されている場合、すべてのアプリケーション SIP インターフェイスは「AAES256-GCM-SHA384:AES256-SHA256」暗号のみをサポートし、[エンタープライズパラメータ (Enterprise Parameter)] の値は無視されます。

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 20: TLS 暗号のためのユニファイドコミュニケーションマネージャーの暗号サポート

| アプリケーション/プロセス | プロトコル | ポート | 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: (注) リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA128-SHA CAMELLIA256-SHA: |

| アプリケーション/プロセス | プロトコル | ポート | サポート対象の暗号方式 |
|---------------|---------|------------|--|
| DRS | TCP/TLS | 4040 | ECDHE-RSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-SHA384: AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-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: DHE-RSA-CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-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-AES256-SHA: ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES128-SHA256: ECDHE-ECDSA-AES128-SHA: ECDHE-RSA-AES256-SHA: (注) リリース 14SU2以降、次の暗号はサポートされていません。 DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA: ECDHE-RSA-DES-CBC3-SHA: EDH-RSA-DES-CBC3-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: |

| アプリケーション/プロセス | プロトコル | ポート | サポート対象の暗号方式 |
|--|---------|------|---|
| Cisco CallManager | TCP/TLS | 5061 | <p>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:</p> <p>(注) リリース 14SU2 以降、次の暗号はサポートされていません。</p> <p>ECDHE-ECDSA-AES256-SHA: CAMELLIA256-SHA: CAMELLIA128-SHA: ECDHE-ECDSA-DES-CBC3-SHA</p> |
| 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 | <p>AES256-GCM-SHA384:AES256-SHA256: AES256-SHA:CAMELLIA256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:CAMELLIA128-SHA:</p> |
| Cisco Certificate Authority Proxy Function | TCP/TLS | 3804 | <p>AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA:</p> <p>(注) リリース 14SU2 以降、次の暗号はサポートされていません。</p> <p>CAMELLIA256-SHA: CAMELLIA128-SHA:</p> |

| アプリケーション/プロセス | プロトコル | ポート | サポート対象の暗号方式 |
|-----------------------------------|---------|------|---|
| 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: (注) リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA |
| シスコ信頼検証サービス | TCP/TLS | 2445 | AES256-GCM-SHA384:AES256-SHA256: AES256-SHA: AES128-GCM-SHA256:AES128-SHA256: AES128-SHA: (注) リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA |
| Cisco Intercluster Lookup Service | 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: (注) リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: |

| アプリケーション/プロセス | プロトコル | ポート | サポート対象の暗号方式 |
|-----------------------|---------|-----------|---|
| 安全な設定ダウンロード (HAPROXY) | TCP/TLS | 6971、6972 | <p>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: AES128-GCM-SHA256:AES128-SHA256: ECDHE-RSA-AES256-SHA:</p> <p>(注) リリース 14SU2 以降、次の暗号はサポートされていません。</p> <p>DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-DES-CBC3-SHA: CAMELLIA128-SHA:</p> |
| 認証済み UDS 連絡先の検索 | TCP/TLS | 9443 | <p>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:</p> <p>(注) リリース 14SU2 以降、次の暗号はサポートされていません。</p> <p>DHE-RSA-CAMELLIA256-SHA: CAMELLIA256-SHA: DHE-RSA-CAMELLIA128-SHA: CAMELLIA128-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-ECDSA-DES-CBC3-SHA:</p> |

表 21 : *Unified Communications Manager IM & Presence* 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 | ポート | サポート対象の暗号方式 |
|-----------------|---------|------|---|
| Cisco SIP Proxy | TCP/TLS | 5061 | <p> 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: (注) リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA: </p> |
| Cisco SIP Proxy | TCP/TLS | 5062 | <p> 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: (注) リリース 14SU2 以降、次の暗号はサポートされていません。 CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA: </p> |

| アプリケーション/プロセス | プロトコル | ポート | サポート対象の暗号方式 |
|-----------------|---------|------|---|
| Cisco SIP Proxy | TCP/TLS | 8083 | <p>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:</p> <p>(注) リリース 14SU2 以降、次の暗号はサポートされていません。</p> <p>CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA:</p> |

| アプリケーション/プロセス | プロトコル | ポート | サポート対象の暗号方式 |
|---------------|---------|----------|---|
| Cisco Tomcat | TCP/TLS | 8443、443 | <p>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:</p> <p>(注) リリース 14SU2以降、次の暗号はサポートされていません。</p> <p>CAMELLIA128-SHA: CAMELLIA256-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: DHE-RSA-CAMELLIA128-SHA: DHE-RSA-CAMELLIA256-SHA: ECDHE-ECDSA-AES256-SHA: EDH-RSA-DES-CBC3-SHA:</p> |

| アプリケーション/プロセス | プロトコル | ポート | サポート対象の暗号方式 |
|--|---------|------|--|
| Cisco XCP XMPP Federation Connection Manager | TCP/TLS | 5269 | <p>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:</p> <p>(注) リリース 14SU2 以降、次の暗号はサポートされていません。</p> <p>CAMELLIA256-SHA: CAMELLIA128-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-RSA-AES256-SHA:</p> |
| Cisco XCP Client Connection Manager | TCP/TLS | 5222 | <p>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:</p> <p>(注) リリース 14SU2 以降、次の暗号はサポートされていません。</p> <p>CAMELLIA128-SHA: CAMELLIA256-SHA: DES-CBC3-SHA: ECDHE-ECDSA-DES-CBC3-SHA: ECDHE-RSA-DES-CBC3-SHA: ECDHE-ECDSA-AES256-SHA: ECDHE-RSA-AES256-SHA:</p> |

表 22: SSH 暗号の暗号サポート

| サービス | 暗号/アルゴリズム |
|---------|---|
| SSH サーバ | <ul style="list-style-type: none"> • 暗号 <ul style="list-style-type: none"> aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC アルゴリズム : <ul style="list-style-type: none"> hmac-sha2-256 hmac-sha2-512 hmac-sha1 • KEX アルゴリズム : <ul style="list-style-type: none"> ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 • 非 FIPS モードのホストキーアルゴリズム : <ul style="list-style-type: none"> rsa-sha2-256 rsa-sha2-512 ssh-rsa • FIPS モードのホストキーアルゴリズム : <ul style="list-style-type: none"> rsa-sha2-256 rsa-sha2-512 |

| サービス | 暗号/アルゴリズム |
|------------|---|
| SSH クライアント | <ul style="list-style-type: none"> • 暗号 : <ul style="list-style-type: none"> aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com • MAC アルゴリズム : <ul style="list-style-type: none"> hmac-sha2-256 hmac-sha2-512 hmac-sha1 • KEX アルゴリズム : <ul style="list-style-type: none"> ecdh-sha2-nistp521 ecdh-sha2-nistp384 ecdh-sha2-nistp256 diffie-hellman-group14-sha1 diffie-hellman-group14-sha256 diffie-hellman-group16-sha512 • 非 FIPS モードのホストキーアルゴリズム : <ul style="list-style-type: none"> rsa-sha2-256 rsa-sha2-512 ssh-rsa • FIPS モードのホストキーアルゴリズム : <ul style="list-style-type: none"> rsa-sha2-256 rsa-sha2-512 |

| サービス | 暗号/アルゴリズム |
|-------------|---|
| DRS クライアント | <ul style="list-style-type: none"> • 暗号 : <ul style="list-style-type: none"> aes256-ctr aes256-cbc aes128-ctr aes128-cbc aes192-ctr aes192-cbc • MAC アルゴリズム : <ul style="list-style-type: none"> hmac-md5 hmac-sha2-256 hmac-sha1 hmac-sha1-96 hmac-md5-96 • KEX アルゴリズム : <ul style="list-style-type: none"> ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group1-sha1 <p>(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-hellman-group-exchange-sha1、および diffie-hellman-group1-sha1 は、リリース 12.5(1)SU4 からサポートされません。暗号が設定されていない場合、DRS クライアントはこれらのアルゴリズムを使用します。</p> |
| SFTP クライアント | <ul style="list-style-type: none"> • 暗号 : <ul style="list-style-type: none"> aes128-ctr aes192-ctr aes256-ctr • MAC アルゴリズム : <ul style="list-style-type: none"> hmac-sha2-256 hmac-sha2-512 hmac-sha1 • KEX アルゴリズム : <ul style="list-style-type: none"> ecdh-sha2-nistp521 ecdh-sha2-nistp384 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 |

| サービス | 暗号/アルゴリズム |
|--------------------------|----------------------|
| エンドユーザ | hmac-sha512 |
| 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 (Cipher Management)] 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:
AECMH-AES256-SHA:AECMH-AES128-SHA:AECMH-DES-CBC3-SHA:AECMH-RC4-SHA:AECMH-NUL-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-NUL-SHA:ECDHE-ECDSA-NUL-SHA:
ECDH-RSA-NUL-SHA:ECDH-ECDSA-NUL-SHA:NULL-SHA256:NULL-SHA
```

SSH 無効暗号

```
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 11 章

電話機のセキュリティ

- [電話のセキュリティの概要 \(145 ページ\)](#)
- [電話セキュリティプロファイル \(158 ページ\)](#)
- [SIP 電話機のダイジェスト認証の概要 \(179 ページ\)](#)

電話のセキュリティの概要

インストール時は、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、電話機を起動すると、デバイスはすべて非セキュアとして Unified Communications Manager に登録されます。

Unified Communications Manager 4.0(1) 以降のリリースからアップグレードした後は、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電話機が起動します。デバイスはすべて、選択されたセキュリティモードを使用して登録されます。

Unified Communications Manager をインストールすると、Unified Communications Manager および TFTP サーバに自己署名証明書が作成されます。自己署名証明書ではなく、Unified Communications Manager のサードパーティの CA 署名付き証明書を使用することもできます。認証を設定した後、Unified Communications Manager は、証明書を使用して、サポートされている Cisco Unified IP Phone で認証します。Unified Communications Manager および TFTP サーバに証明書が存在した後、Unified Communications Manager は各 Unified Communications Manager アップグレード中に証明書を再発行しません。CLI コマンド `ctl update CTLFile` を使用して、ctl ファイルを新しい証明書エントリで更新する必要があります。



ヒント サポートされていない、または非セキュアなシナリオについては、連携動作と制限事項に関連するトピックを参照してください。

Unified Communications Manager は認証および暗号化のステータスをデバイスレベルで維持します。コールに関係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、コールステータスはセキュアとして登録されます。一方のデバイスが非セキュアとして登録されている場合、発信者または受信者の電話機がセキュアとして登録されていても、コールは非セキュアとして登録されます。

Unified Communications Manager では、ユーザが Cisco Extension Mobility を使用している場合、デバイスの認証と暗号化のステータスは保持されます。また、Unified Communications Manager では、共有回線が設定されている場合、デバイスの認証と暗号化のステータスも保持されます。



ヒント 暗号化された Cisco IP 電話に対して共有回線を設定するときには、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。

電話機のセキュリティ強化の概要

このセクションでは、 Gratuitous ARP 無効化、 Web アクセス無効化、 PC 音声 VLAN アクセス無効化、アクセス無効化設定、 PC ポート無効化など、電話機のセキュリティ強化動作の概要を説明します。

Cisco IP 電話への接続のセキュリティを強化するために、次のオプション設定を使用します。これらの設定は、[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)] に表示されます。

これらを企業全体の一連の電話機またはすべての電話機に適用するには、[共通電話プロファイルの設定 (Common Phone Profile Configuration)] ウィンドウおよび [エンタープライズ電話の設定 (Enterprise Phone Configuration)] にもこれらの設定が表示されます。

表 23: 電話機のセキュリティ強化の動作

| 電話機のセキュリティ強化の動作 | 説明 | |
|----------------------------|--|--|
| <p>Gratuitous ARP の無効化</p> | <p>デフォルトでは、Cisco Unified IP 電話 s は ARP パケットを受け入れます。デバイスが使用する Gratuitous ARP パケットは、ネットワークにデバイスの存在を公表するために使用されます。ただし、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をスプーフィングすることができます。たとえば、攻撃者は、デフォルトルータであると主張するパケットを送信する可能性があります。これを選択した場合は、[電話の設定 (Phone Configuration)] ウィンドウで、無償 ARP を無効にすることができます。</p> <p>(注) この機能を無効にしても、電話機がデフォルトルータを特定することはできません。</p> | |

| 電話機のセキュリティ強化の動作 | 説明 | |
|-----------------|--|--|
| Web アクセスの無効化 | <p>電話の Web サーバ機能を無効にすると、統計および設定情報を提供する電話内部の Web ページへのアクセスがブロックされます。Cisco Quality Report Tool などの機能は、電話の Web ページにアクセスしないと正しく動作しません。また、Web サーバを無効にすると、CiscoWorks など、Web アクセスに依存するサービスアビリティアプリケーションにも影響します。</p> <p>Web サービスが無効になっているかどうかを確認するために、電話機は設定ファイルのパラメータを解析して、サービスが無効になっているか、有効になっているかを示します。Web 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目的で HTTP ポート80を開かず、電話機の内部 web ページへのアクセスをブロックします。</p> | |

| 電話機のセキュリティ強化の動作 | 説明 | |
|-----------------------|--|--|
| PC 音声 VLAN へのアクセスの無効化 | <p>デフォルトでは、Cisco IP 電話はスイッチポート（上流に位置するスイッチに面したポート）で受信したすべてのパケットを PC ポートに転送します。[Phone Configuration] ウィンドウの [PC Voice VLAN Access] 設定を無効にすると、PC ポートから受信した音声 VLAN 機能を使用するパケットはドロップされます。さまざまな Cisco IP 電話がそれぞれ異なる方法でこの機能を使用しています。</p> <ul style="list-style-type: none"> • Cisco Unified IP 電話 7942 と 7962 は、PC ポートで送受信される、音声 VLAN のタグが付いたパケットをドロップします。 • Cisco Unified IP 電話 7970G は、PC ポートで送受信される、VLAN で 802.1Q のタグが含まれるすべてのパケットをドロップします。 | |

| 電話機のセキュリティ強化の動作 | 説明 | |
|-----------------|---|--|
| アクセスの無効化の設定 | <p>デフォルトでは、Cisco IP 電話の [Applications] ボタンを押すと、電話の設定情報を含むさまざまな情報にアクセスできます。[Phone Configuration] ウィンドウで [Setting Access] パラメータ設定を無効にすると、通常は電話の [Applications] ボタンを押すと表示されるすべてのオプション ([Contrast]、[Ring Type]、[Network Configuration]、[Model Information]、[Status] などの設定) へのアクセスが拒否されます。</p> <p>Unified Communications Manager Administration 内の設定を無効にすると、以前の設定は電話に表示されません。この設定を無効にすると、電話ユーザは [音量 (Volume)] ボタンに関連付けられている設定を保存できません。たとえば、ユーザはボリュームを保存できません。</p> <p>この設定を無効にすると、現在のコントラスト、呼出音タイプ、ネットワーク設定、モデル情報、ステータス、および電話機に存在するボリューム設定が自動的に保存されます。これらの電話機設定を変更するには、Unified Communications Manager Administration で [設定へのアクセス (Setting Access)] 設定を有効にします。</p> | |

| 電話機のセキュリティ強化の動作 | 説明 | |
|-----------------|--|--|
| PC ポートのディセーブル化 | <p>デフォルトでは、Unified Communications Manager は PC ポートを備えているすべての Cisco IP 電話で PC ポートを有効にします。これを選択した場合は、[電話の設定 (Phone Configuration)] ウィンドウで [PC ポート (PC Port)] 設定を無効にすることができます。PC ポートを無効にすると、ロビーまたは会議室の電話機で役立ちます。</p> <p>(注) PC ポートは一部の電話機で使用でき、ユーザは電話機にコンピュータを接続できます。この接続方法は、ユーザが1つの LAN ポートだけを必要とすることを意味します。</p> | |

電話のセキュリティ強化の設定

電話のセキュリティ強化は、接続のセキュリティを強化するために電話機に適用できるオプションの設定で構成されています。次の3つの設定ウィンドウのいずれかを使用して設定を適用できます。

- 電話の設定 - [電話の設定 (Phone Configuration)] 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 (Common Phone Profile)] 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機に設定を適用します。
- 企業電話 - [企業電話 (Enterprise Phone)] ウィンドウを使用して、企業全体のすべての電話機に設定を適用します。



(注) これらの各ウィンドウに競合する設定が表示される場合、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) 企業電話。

電話のセキュリティ強化を設定するには、次の手順を実行します。

- ステップ 1** Cisco Unified Communications Manager Administrationから、[デバイス (Device)] > [電話 (Phone)] を選択します。
- ステップ 2** 電話機の検索条件を指定して [検索 (Find)] をクリックし、すべての電話機を表示します。
- ステップ 3** デバイス名をクリックします。
- ステップ 4** 次の製品固有のパラメータを見つけます。
- [PC ポート (PC Port)]
 - [設定アクセス (Settings Access)]
 - [無償 ARP (Gratuitous ARP)]
 - [PC の音声 VLAN へのアクセス (PC Voice VLAN Access)]
 - [Web アクセス (Web Access)]
- ヒント** これらの設定の情報を確認するには、[電話の設定 (Phone Configuration)] ウィンドウのパラメータの横に表示される [ヘルプ (help)] アイコンをクリックします。
- ステップ 5** 無効にする各パラメータのドロップダウンリストから、[無効 (Disabled)] を選択します。スピーカフォンまたはスピーカ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オンにします。
- 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 では Cisco IP 電話の電話モデルによって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、コールがセキュアであるかどうか、接続されたデバイスが信頼できるかどうかを示します。

信頼できるデバイスとは、シスコ製デバイスか、シスコの信頼される接続のセキュリティ基準に合格したサードパーティ製デバイスを表します。これには、シグナリングおよびメディア暗号化、プラットフォームハードニング、保証などがあります。デバイスが信頼できる場合、セキュリティアイコンが表示され、サポートされるデバイスでセキュアトーンが再生されます。さらに、デバイスはセキュアコールに関する他の機能やインジケータも備えていることがあります。

デバイスをシステムに追加すると、Unified Communications Manager は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目的でだけ表示され、管理者は直接設定できません。

Unified Communications Manager はアイコンおよびメッセージを Unified Communications Manager Administration に表示することでゲートウェイが信頼できるかを示します。

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デバイスのセキュリティ アイコンの動作について説明します。

Cisco Unified Communications Manager の管理

[Unified Communications Manager Administration] の次のウィンドウには、デバイスが信頼されているかどうかが表示されます。

[Gateway Configuration]

ゲートウェイ タイプごとに、[Gateway Configuration] ウィンドウ ([Device] > [Gateway]) には、[Device Is Trusted] または [Device Is Not Trusted] と対応するアイコンが表示されます。

システムはデバイスタイプに基づいて、デバイスが信頼できるかどうかを判断します。ユーザはデバイスが信頼できるかどうかを設定できません。

[Phone Configuration]

電話デバイス タイプごとに、[Phone Configuration] ウィンドウ ([Device] > [Phone]) に [Device Is Trusted] または [Device Is Not Trusted] と対応するアイコンが表示されます。

システムはデバイスタイプに基づいて、デバイスが信頼できるかどうかを判断します。ユーザはデバイスが信頼できるかどうかを設定できません。

デバイスが信頼決定基準と呼ばれる

ユーザがコール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つの基準に基づいて、コールがセキュアであるかどうかを判定します。

- コールのすべてのデバイスが信頼できるか。
- シグナリングはセキュア（認証されていて暗号化されている）か。
- メディアはセキュアか。

サポート対象の Cisco Unified IP Phone にロック セキュリティアイコンが表示される前に、これら3つの基準がすべて満たされている必要があることに注意してください。信頼できないデバイスを含むコールでは、シグナリングおよびメディアのセキュリティに関係なく、コール全体のステータスはセキュアでないままで、電話機にロックアイコンが表示されません。たとえば、会議で信頼できないデバイスを含めた場合、システムは、そのコールレグと会議自体をセキュアでないものと見なします。

電話機モデルのサポート

Unified Communications Manager でセキュリティをサポートする電話モデルは、セキュアなシスコの電話とセキュアな推奨ベンダーの電話という2つのカテゴリに分類されます。セキュアなシスコの電話機には、製造元でインストールされる証明書(MIC)が事前にインストールされて

おり、認証局プロキシ機能 (CAPF) を使用して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。セキュアなシスコの電話機は、追加の証明書の管理なしで MIC を使用して Cisco ユニファイド CM に登録できます。セキュリティを強化するために、CAPF を使用して電話機に LSC を作成してインストールすることができます。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連するトピックを参照してください。

セキュアな推奨ベンダーの電話機には、MIC が事前にインストールされておらず、LSCs を生成するための CAPF がサポートされていません。セキュアな推奨ベンダーの電話機が Cisco ユニファイド CM に接続するためには、デバイスに証明書を提供するか、デバイスによって生成される必要があります。電話機のサプライヤは、電話機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 管理証明書管理インターフェイスを使用して Cisco ユニファイド 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、推奨ベンダーの SIP 電話のセキュリティ設定に関連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るセキュリティ機能のリストについては、この Unified Communications Manager リリースに対応した電話管理およびユーザマニュアル、またはファームウェアロードに対応したファームウェアのマニュアルを参照してください。

また、シスコのユニファイドレポートを使用して、特定の機能をサポートしている電話機を一覧表示することもできます。Cisco Unified Reporting の詳細については、『Cisco Unified Reporting Administration Guide』を参照してください。

電話機の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機の特定のセキュリティ関連の設定を構成して表示することができます。たとえば、電話機にローカルで有効な証明書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。セキュアメニューとアイコンの詳細については、ご使用の電話モデルに対応する Cisco IP 電話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。

Unified Communications Manager がコールを認証済みまたは暗号化済みと分類すると、コール状態を示すアイコンが電話に表示されます。Unified Communications Manager がどの時点でコールを認証済みまたは暗号化済みとして分類するかも決定します。

電話機のセキュリティの設定

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。

- ステップ 1 Cisco CTL クライアントが設定されていない場合は、**utils ctl CLI** コマンドを実行し、Unified Communications Manager のセキュリティモードが混合モードであることを確認します。
- ステップ 2 電話機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は、Certificate Authority Proxy Function (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 電話に電話セキュリティプロファイルを適用します。

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 (Phone Configuration)] 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 Phone 7962 または 7942 (SIP のみ) で、[エンドユーザ設定 (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名とパスワード (ダイジェストログイン情報) を入力します。

(注) このドキュメントでは、電話へのダイジェスト認証クレデンシャルの入力方法は説明していません。このタスクの実行方法については、お使いの電話機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』およびこのバージョンの Unified Communications Manager 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後、`utils ctl` CLI コマンドセットを実行して CTL ファイルを更新する必要があります。

ステップ 7 電話機がこの機能をサポートしている場合は、電話機の設定ファイルを暗号化します。

ステップ 8 電話機を強化するには、電話機の設定を無効にします。

推奨ベンダーの SIP 電話セキュリティのセットアップ

推奨ベンダーのセキュアな電話とは、サードパーティベンダーによって製造されているが、COP ファイルを使用して Cisco Unified データベースにインストールされている電話です。推奨ベンダーの SIP 電話のセキュリティは、Unified Communications Manager が提供しています。セキュリティをサポートするためには、COP ファイル内の推奨ベンダーの SIP 電話の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 (Add a New Phone)] ウィンドウのドロップダウンリストに表示されます。すべての推奨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、すべての推奨ベンダーの電話が TLS セキュリティをサポートするわけではありません。セキュリティ機能は、電話機のモデルに基づいています。電話セキュリティプロファイルに「[Device Security Mode]」フィールドが含まれる場合、電話は TLS をサポートしています。

推奨ベンダーの電話機が TLS セキュリティをサポートしている場合は、デバイスごとの証明書と共有証明書の2つのモードが考えられます。電話機のサプライヤは、電話機に適用されるモード、および電話機の証明書の生成または取得の手順を指定する必要があります。

推奨ベンダーの SIP 電話セキュリティプロファイルのデバイスごとの証明書の設定

デバイスごとの証明書を使用して推奨ベンダーの 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。

ステップ 1 OS 管理証明書管理インターフェイスを使用して、各電話機の証明書をアップロードします。

ステップ 2 [Cisco Unified Administration] で、[System] > [Security] > [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対して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 (Device Security Mode)] ドロップダウンリストで [暗号化 (Encrypted)] または [認証済み (Authenticated)] 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、[デバイス (Device)] > [電話 (Phone)] > [追加 (Add new)] の順に選択します。
- ステップ5 [Phone Type] 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 [デバイスの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で、作成したプロファイルを選択します。

推奨ベンダーの 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

共有証明書を使用して推奨ベンダーの 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。

- ステップ1 電話機のベンダーの指示を使用して、サブジェクト代替名 (SAN) 文字列を使用して証明書を生成します。SAN のタイプは DNS である必要があります。この手順で指定した SAN をメモしておきます。たとえば、X509v3 extensions の場合は次のようになります。
- 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。または、セキュリティが有効になっていません。
- ステップ2 OS 管理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 Administration] で、[System] > [Security] > [Phone Security Profile] の順に選択します。
- ステップ4 [名前 (name)] フィールドにサブジェクト代替名 (san) の名前を入力します。これは、優先ベンダーから提供された証明書の名前です。または、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 と完全に一致する必要があります。そうしないと、セキュリティが有効になりません。
- ステップ5 [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で、[暗号化 (Encrypted)] または [認証済み (Authenticated)] を選択します。
- ステップ6 [転送タイプ (Transport type)] ドロップダウンリストで、[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、[デバイス (Device)] > [電話 (Phone)] > [追加 (Add new)] の順に選択します。
- ステップ8 [Phone Type] を選択します。
- ステップ9 各必須フィールドに入力します
- ステップ10 [デバイスの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で、作成したプロファイルを選択します。

クラスタ間での電話の移行

クラスタ間で電話を移動するには、次の手順に従ってください。たとえば、クラスタ1からクラスタ2に移動するとします。

- ステップ1 クラスタ2で、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 (Find)] をクリックします。
 - ステップ3 証明書の一覧で、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することにより、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 証明書の一覧で、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することにより、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 クラスタ1で、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6 [証明書チェーンのアップロード (Upload Certificate Chain)] をクリックすることにより、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、[電話と SAST 間の信頼 (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)] フィールドで、[ファイルの選択 (Choose File)] をクリックし、手順3でダウンロードした ITLRecovery ファイルを参照し、[ファイルのアップロード (Upload File)] をクリックします。
アップロードされた ITLRecovery ファイルが、クラスタ1の [証明書リスト (Certificate List)] ウィンドウで [電話と SAST 間の信頼 (Phone-SAST-Trust)] 証明書に対して表示されます。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 証明書をクラスタ2の CAPF 信頼ストアにアップロードしなければなりません。
 - ステップ10 (任意) この手順は、クラスタが混合モードの場合にのみ適用可能です。CLI で `utils ctl update CTLFile` コマンドを実行することにより、CTL ファイルをクラスタ1で再生成します。
(注)
 - `show ctl` CLI コマンドを実行することにより、クラスタ2の ITLRecovery 証明書と CallManager 証明書が、SAST としての役割で CTL ファイルに含まれるようにします。
 - 電話が新しい CTL ファイルおよび ITL ファイルを受け取っていることを確認します。更新された CTL ファイルには、クラスタ2の ITLRecovery 証明書が含まれています。
- クラスタ1からクラスタ2に移行する電話が、クラスタ2の ITLRecovery 証明書を受け付けるようになります。
- ステップ11 クラスタ間で電話を移行します。

電話セキュリティの連携動作と制限事項

ここでは、電話機のセキュリティに関する対話と制限について説明します。

表 24: 電話セキュリティの連携動作と制限事項

| 機能 | 連携動作および制限事項 |
|---------|--|
| 証明書の暗号化 | <p>Unified Communications Manager リリース 11.5(1)SU1 から、CAPF サービスで発行されるすべての LSC 証明書は SHA-256 アルゴリズムで署名されます。したがって、Cisco Unified IP Phone 7900 シリーズ、8900 シリーズ、および 9900 シリーズは、SHA-256 で署名された LSC 証明書および外部 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。</p> <p>(注) ソフトウェアメンテナンスが終了した電話モデルまたはサポート終了電話モデルを使用する場合は、Unified Communications Manager 11.5(1)SU1 リリースより前のバージョンを使用することを推奨します。</p> |

電話セキュリティプロファイル

Unified Communications Manager で、電話機のタイプとプロトコルのセキュリティ関連の設定をセキュリティプロファイルにグループ分けします。したがって、この1つのセキュリティプロファイルを複数の電話機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、いくつかの CAPF 設定などがあります。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。

[電話の設定 (Phone Configuration)] 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、構成済みの設定を電話に適用します。電話機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に応じた新しいセキュリティプロファイルを設定してから、そのプロファイルを電話機に適用する必要があります。選択されたデバイスとプロトコルがサポートするセキュリティ機能のみが、[セキュリティプロファイルの設定 (security profile settings)] 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。

- 電話を設定するときは、[電話の設定 (Phone 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。デバイスがセキュリティまたはセキュアプロファイル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適用します。

- 事前定義された非セキュアプロファイルを削除または変更することはできません。
- デバイスに現在割り当てられているセキュリティプロファイルは削除できません。
- すでに電話機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、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、再設定された設定が適用されます。
- 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機は、新しいプロファイル名と設定を前提としています。
- CAPF 設定、認証モード、およびキーサイズは、[電話の設定 (Phone Configuration)] ウィンドウに表示されます。Mic または LSCs に関連する証明書操作の 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、[電話の設定 (Phone Configuration)] 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の CAPF 設定を更新すると、[電話の設定 (Phone Configuration)] ウィンドウ上の設定も同様に更新されます。
- [電話の設定 (Phone Configuration)] 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った場合、Unified Communications Manager は一致するプロファイルを電話機に適用します。
- [電話の設定 (Phone Configuration)] 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かった場合、Unified Communications Manager は新しいプロファイルを作成してそのプロファイルを電話機に適用します。
- アップグレード前にデバイスセキュリティ モードを設定済みの場合は、Unified Communications Manager が設定済みのモデルとプロトコルに基づいてプロファイルを作成し、デバイスにそのプロファイルを適用します。
- MIC は LSC のインストール時にのみ使用することを推奨します。シスコでは、Unified Communications Manager との TLS 接続の認証用に LSC をサポートしています。MIC ルート証明書は侵害される可能性があるため、TLS 認証またはその他の目的に MIC を使用するように電話を設定するユーザは、ご自身の責任で行ってください。MIC が侵害された場合シスコはその責任を負いません。
- TLS 接続に LSC を使用するには、Cisco IP 電話をアップグレードし、互換性の問題を回避するために MIC ルート証明書を CallManager 信頼ストアから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

次の表では、SCCP を実行している電話のセキュリティプロファイルに関する設定について説明します。

選択した電話のタイプおよびプロトコルがサポートする設定のみ表示します。

表 25: 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 | <p>セキュリティ プロファイルの名前を入力します。</p> <p>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 [デバイスのセキュリティ 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。</p> <p>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、プロファイルの検索または更新時に正しいプロファイルを検索できます。</p> |
| [説明 (Description)] | <p>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、任意の言語で最大 50 文字を指定できますが、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。</p> |

| 設定 | 説明 |
|---|----|
| [デバイスセキュリティモード (Device Security Mode)] | |

| 設定 | 説明 |
|----|---|
| | <p>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。</p> <ul style="list-style-type: none"> • [非セキュア (Non Secure)] : イメージ、ファイル、デバイス認証を除くセキュリティ機能は電話機に存在しません。TCP 接続で Unified Communications Manager が利用できます。 • [認証済 (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、認証、およびシグナリング暗号化を提供します。 <p>説明したように、次の暗号方式がサポートされています。</p> <p>TLS暗号方式</p> <p>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。</p> <p>最も強力 : AES-256 SHA-384 のみ : RSA 優先</p> <ul style="list-style-type: none"> • TLS_ECDHE_RSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 <p>(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。</p> <p>最も強力 : AES-256 SHA-384 のみ : ECDSA 優先</p> <ul style="list-style-type: none"> • TLS_ECDHE_ECDSA with AES256_GCM_SHA384 • TLS_ECDHE_RSA with AES256_GCM_SHA384 <p>中 - AES-256 AES-128のみ: RSA優先</p> <p>(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。</p> <ul style="list-style-type: none"> • 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 |
|----|---|
| | <ul style="list-style-type: none"> • TLS_ECDHE_ECDSA with AES128_GCM_SHA256 <p>(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。</p> <p>中程度 : AES-256 AES-128 のみ : ECDSA 優先</p> <ul style="list-style-type: none"> • 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 <p>(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。</p> <p>すべての暗号方式: RSA優先</p> <ul style="list-style-type: none"> • 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 <p>すべての暗号 ECDSA 優先</p> <ul style="list-style-type: none"> • 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 |
|-------------------------|--|
| | <ul style="list-style-type: none"> • TLS_RSA with AES_128_CBC_SHA1 <p>(注) [認証済み (Authenticated)]として選択されている [デバイスセキュリティプロファイル (Device Security Profile)] を使用してトランクを設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS 接続 (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。</p> |
| [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 |
|----|--|
| | <p>このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。</p> <p>ドロップダウンリストボックスから、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> • [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/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/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。 <p>このオプションでは、セキュリティは提供されません。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。</p> <ul style="list-style-type: none"> • [By Existing Certificate (Precedence to LSC)] : 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) が電話に存在する場合に、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、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、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に MIC と LSC が存在する場合、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。 <p>このオプションを選択する前に、電話機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て、電話機に証明書が存在しない場合、操作は失敗します。</p> <p>MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。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。</p> <ul style="list-style-type: none"> • [By Existing Certificate (Precedence to MIC)] : 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/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、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 <p>このオプションを選択する前に、電話機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て、電話機に証明</p> |

| 設定 | 説明 |
|--|--|
| | <p>書が存在しない場合、操作は失敗します。</p> <p>(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 パラメータと連携します。</p> |
| <p>[キーの順序 (Key Order)]</p> | <p>このフィールドは、CAPF のキーの順序を指定します。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。</p> <ul style="list-style-type: none"> • [RSA のみ (RSA Only)] • [ECのみ (EC Only)] • [EC 優先、RSA バックアップ (EC Preferred, RSA Backup)] <p>(注) [Key Order]、[RSA Key Size]、および [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。[EC Only]値を選択し、[EC Key Size] の値を [256] ビットにすると、デバイスセキュリティプロファイルには値 EC-256 が付加されます。</p> |
| <p>[RSA Key Size (Bits)]</p> | <p>ドロップダウンリストボックスから、[512]、[1024]、[2048]、[3072]、または4096 のいずれかの値を選択します。</p> <p>(注) CallManager が [Certificate Purpose] で選択した RSA の [key length] が 2048 より大きいと、一部の電話モデルが登録に失敗する場合があります。Cisco Unified Reporting Tool (CURT) の [Unified CM Phone Feature List Report] で、3072/4096 RSA キーサイズサポート機能をサポートする電話モデルの一覧を確認できます。</p> |
| <p>[ECキーサイズ (ビット) (EC Key Size (Bits))]</p> | <p>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。</p> |

次の表では、SIP を実行している電話のセキュリティプロファイルに対する設定について説明します。

表 26: SIP 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 | <p>セキュリティ プロファイルの名前を入力します。</p> <p>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 [デバイスのセキュリティ 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。</p> <p>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、プロファイルの検索または更新時に正しいプロファイルを検索できます。</p> |
| [説明 (Description)] | 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)] | <p>ナンス値が有効な分数 (秒単位) を入力します。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。</p> <p>(注) ナンス値は、ダイジェスト認証をサポートする乱数であり、ダイジェスト認証パスワードの MD5 ハッシュを計算するときに使用されます。</p> |

| 設定 | 説明 |
|---|---|
| [デバイスセキュリティモード (Device Security Mode)] | <p>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。</p> <ul style="list-style-type: none"> • [非セキュア (Non Secure)]: イメージ、ファイル、デバイス認証を除くセキュリティ機能は電話機に存在しません。TCP 接続で Unified Communications Manager が利用できます。 • [認証済 (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。シグナリングに AES128/SHA を使用する TLS 接続が開き、SRTP はすべての SRTP 対応ホップでのすべてのコールに対してメディアを伝送します。 <p>(注) [認証済み (Authenticated)]として選択されている [デバイスセキュリティプロファイル (Device Security Profile)]を使用してトランクを設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS 接続 (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。</p> |

| 設定 | 説明 |
|---|---|
| 転送タイプ | <p>[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)。</p> <ul style="list-style-type: none"> • [TCP] : Transmission Control Protocol を選択し、パケットが送信したときと同じ順序で受信されるようにします。このプロトコルを使用すると、パケットはドロップされませんが、プロトコルはセキュリティを提供しません。 • [UDP] : User Datagram Protocol を選択し、パケットがすばやく受信されるようにします。このプロトコルはパケットをドロップする可能性があり、パケットは送信された順序で受信されない場合があります。このプロトコルはセキュリティを提供しません。 • [TCP + UDP] : TCP と UDP を組み合わせて使用する場合は、このオプションを選択します。このオプションはセキュリティを提供しません。 <p>[デバイスセキュリティモード (Device Security Mode)] が [認証 (Authenticated)] または [暗号化 (Encrypted)] の場合、TLS では [転送タイプ (Transport Type)] を指定します。TLS は、SIP 電話に対してシグナリングの整合性、デバイス認証、およびシグナリング暗号化 (暗号化モードに限る) を提供します。</p> <p>プロファイルで [デバイスセキュリティモード (Device Security Mode)] を設定できない場合は、転送タイプとして UDP を指定します。</p> |
| [ダイジェスト認証の有効化 (Enable Digest Authentication)] | <p>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。</p> <p>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、認証または暗号化のセキュリティモードを選択します。</p> |
| TFTP 暗号化 (TFTP Encrypted Config) | <p>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ファイルを暗号化します。このオプションはシスコ製電話機に限り使用できます。</p> <p>ヒント このオプションを有効にして、対称キーを設定し、ダイジェストログイン情報と管理者パスワードを保護することをお勧めします。</p> |

| 設定 | 説明 |
|--|---|
| [OAuth 認証の有効化 (Enable OAuth Authentication)] | <p>[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 (Encrypted)] を選択すると、このチェックボックスが使用可能になります。</p> <p>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ります。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。</p> <p>SIP OAuth を有効にするには、次のようにします。</p> <ul style="list-style-type: none"> • [Transport Type] が [TLS] の場合 : • [デバイスセキュリティモード (Device Security Mode)]は [暗号化 (Encrypted)]です。 • ダイジェスト認証の無効化 • 暗号化設定は無効です。 <p>(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。</p> |
| [Exclude Digest Credentials in Configuration File] | <p>このチェックボックスをオンにすると、Unified Communications Manager は電話機が TFTP サーバからの電話ダウンロードのダイジェストログイン情報を削除します。このオプションは、Cisco IP 電話、7942、および 7962 (SIP のみ) に対応しています。</p> |

| 設定 | 説明 |
|--------------------------------------|----|
| [認証モード (Authentication Mode)] | |

| 設定 | 説明 |
|----|--|
| | <p>このフィールドでは、電話機が CAPF 証明書の操作時に使用する認証方法を選択できます。このオプションはシスコ製電話機に限り使用できます。</p> <p>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。</p> <ul style="list-style-type: none"> • [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/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/アップグレード、またはトラブルシューティングします。 <p>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。</p> <ul style="list-style-type: none"> • [By Existing Certificate (Precedence to LSC)] : 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) が電話に存在する場合に、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、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、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に LSC が存在しないが、MIC が存在する場合、MIC によって認証が行われます。 <p>このオプションを選択する前に、電話機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て、電話機に証明書が存在しない場合、操作は失敗します。</p> <p>MIC と LSC が同時に電話機に存在できる場合でも、電話機が CAPF への認証に使用する証明書は常に 1 つだけです。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。</p> <ul style="list-style-type: none"> • [By Existing Certificate (Precedence to MIC)] : 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/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、電話機に MIC が存在するかどうかに関係なく、LSC によって認証が行われます。電話機に LSC が存在するが、MIC が存在しない場合、LSC によって認証が行われます。 <p>このオプションを選択する前に、電話機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て、電話機に証明</p> |

| 設定 | 説明 |
|----------------------------|--|
| | 書が存在しない場合、操作は失敗します。 (注) [電話セキュリティプロファイル (Phone Security Profile)] ウィンドウで設定される CAPF 設定は、[電話の設定 (Phone Configuration)] ウィンドウで設定される CAPF パラメータと連携します。 |
| [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。キーサイズのもう 1 つのオプションは、512 です。 デフォルトの設定より大きいキーサイズを選択すると、電話機でキーの生成に必要なエントロピーを生成するのに時間がかかります。キーの生成を低い優先順位で設定すると、操作の実行中に、電話機が機能します。電話機のモデルによっては、キーの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 パラメータと連携します。 |
| 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 を使用して Unified Communications Manager からの SIP メッセージをリッスンする Cisco Unified IP Phone (SIP のみ) の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 を使用している電話機はこの設定を無視します。 |

電話のセキュリティの設定タスクフロー

電話機のセキュリティを設定するには、次のタスクを実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|-------------------------------------|
| ステップ 1 | (任意) 電話セキュリティプロファイルの検索 (175 ページ) | 電話機を保護するために、電話機のセキュリティプロファイルを検索します。 |
| 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 | 電話機を保護するために、電話機のセキュリティプロファイルを設定します。 |
| ステップ 3 | 電話機へのセキュリティプロファイルの適用 | 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。 |

| | コマンドまたはアクション | 目的 |
|--------|------------------------------------|--|
| ステップ 4 | Sip トランクセキュリティプロファイルと SIP トランクの同期 | 選択した電話機とすべての電話セキュリティプロファイルを同期します。 |
| 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ている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 | 電話機のセキュリティプロファイルを使用した電話機の検索 | 電話のセキュリティプロファイルに関連付けられている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インタラクションと制限事項 | SIP トランクセキュリティプロファイルのインタラクションと制限事項 |

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。

- ステップ 1** Cisco Unified Communications Manager Administration で、[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** データベース内のレコードをすべて表示するには、ダイアログボックスを空欄のままにして、[ステップ 3 \(175 ページ\)](#) に進みます。
- レコードをフィルタまたは検索するには、次の手順を実行します。
- 最初のドロップダウンリストで、検索パラメータを選択します。
 - 2 番目のドロップダウンリストで、検索パターンを選択します。
 - 必要に応じて、適切な検索テキストを指定します。
- (注) 検索条件をさらに追加するには、[+] ボタンをクリックします。条件を追加すると、指定した条件をすべて満たしているレコードが検索されます。条件を削除するには、[-] ボタンをクリックして最後に追加された条件を削除するか、または[フィルタのクリア (Clear Filter)] をクリックして、追加されたすべての検索条件を削除します。
- ステップ 3** [検索 (Find)] をクリックします。
- 条件を満たしているレコードがすべて表示されます。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** 表示されるレコードのリストで、表示するレコードのリンクをクリックします。
- (注) ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

ウィンドウに、選択したレコードが表示されます。

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設定するには、次の手順を実行します。

ステップ 1 Cisco Unified Communications Manager Administration で、[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。

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 (Add New)] 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検索し、コピーするセキュリティプロファイルの横にある [コピー (Copy)] ボタン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。

[AddNew] をクリックすると、各フィールドにデフォルト設定が入力された設定ウィンドウが表示されます。[コピー (Copy)] をクリックすると、コピーした設定が入力された設定ウィンドウが表示されます。

ステップ 3 SCCP または SIP を実行している電話機の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。

電話機へのセキュリティプロファイルの適用

電話機の認証に証明書を使用するセキュリティプロファイルを適用する前に、特定の電話機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有効にするには、デバイスタイプとプロトコルに応じた新しいセキュリティプロファイルを設定し、電話機に適用する必要があります。ただし、電話機に証明書が含まれていない場合は、次のタスクを実行します。

- [電話の設定 (Phone Configuration)] ウィンドウで、非セキュアプロファイルを適用します。
- [電話の設定 (Phone Configuration)] ウィンドウで、capf 設定を構成することによって証明書をインストールします。
- [電話の設定 (Phone Configuration)] ウィンドウで、認証または暗号化用に設定されたデバイスセキュリティプロファイルを適用します。

デバイスに電話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。

-
- ステップ 1** [電話の設定 (Phone Configuration)] 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** [Device Security Profile] ドロップダウンリストから、デバイスに適用するセキュリティプロファイルを選択します。
電話機タイプとプロトコルに対してのみ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** 該当する電話に変更を適用するには、[設定の適用 (Apply Config)] 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、[Find And List] ウィンドウで該当するセキュリティプロファイルの横にあるチェックボックスをオンにし、[delete Selected] をクリックします。
-

電話機のセキュリティプロファイルと電話機の同期

電話セキュリティプロファイルに複数の電話を同期させるには、次の手順を実行します。

- ステップ 1** [Unified Communications Manager Administration] で、[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。
- 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。
検索条件に一致する電話セキュリティプロファイルの一覧がウィンドウに表示されます。
- ステップ 3** 該当する電話機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 (Apply Configuration Information)] 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 でセキュリティ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、該当プロファイルを使用するすべてのデバイスを削除してください。

プロファイルを使用するデバイスを確認するには、ステップ 1 を実行します。

- 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)] ドロップダウンリストから [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。

依存関係レコード機能がシステムで有効になっていない場合は、[システム]>[エンタープライズパラメータ設定 (system Enterprise Parameters Configuration)] に移動し、[依存関係レコードの有効化 (Enable dependency Records)] 設定を [True] に変更依存関係レコード機能に関連する高 CPU 使用率に関する情報がメッセージに表示されます。依存関係レコードを有効にするには、変更を保存します。依存関係レコードの詳細については、『Cisco Unified Communications Manager システム設定ガイド』を参照してください。

ここでは、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検索します。
- ステップ 3 複数のセキュリティプロファイルを削除するには、[Find And List] ウィンドウで該当するチェックボックスの横にあるチェックボックスをオンにします。次に、[Delete Selected] をクリックします。この選択で設定可能なすべてのレコードを削除するには、[すべて選択 (Select All)] をクリックして、[選択項目の削除 (Delete Selected)] をクリックします。
- 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、次のいずれかの作業を行います。
 - a) [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横にあるチェックボックスをオンにします。次に、[Delete Selected] をクリックします。
- ステップ 5 削除操作を確認するプロンプトが表示されたら、[OK] をクリックして削除するか、[Cancel] をクリックして削除の操作をキャンセルします。

電話機のセキュリティプロファイルを使用した電話機の検索

特定のセキュリティプロファイルを使用する電話機を検索するには、次の手順を実行します。

- ステップ 1 Cisco Unified Communications Manager Administration から、[デバイス (Device)] > [電話 (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 (Security Profile)] を選択します。
 - a) ドロップダウンリストで、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) 追加の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、指定した条件をすべて満たしてい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、[-] 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、[Clear Filter] をクリックします。
- ステップ 3 [検索 (Find)] をクリックします。

条件を満たしているレコードがすべて表示されます。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 表示されるレコードのリストで、表示するレコードのリンクをクリックします。
 - (注) ソート順を反転させるには、リスト見出しの上矢印または下矢印が使用可能であればそれをクリックします。

ウィンドウに、選択したレコードが表示されます。

SIP トランク セキュリティ プロファイルのインタラクションと制限事項

次の表に、SIP トランク セキュリティ プロファイルの機能の連携動作と制限事項を示します。

表 27: SIP トランク セキュリティ プロファイルのインタラクションと制限事項

| 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 [エクスポート管理された機能を許可 (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 電話機のダイジェスト認証の概要

ダイジェスト認証を使用すると、Unified Communications Manager は SIP を実行している電話機の要求メッセージをチャレンジできます。これには、キーブアライブを除くすべての要求メッセージが含まれます。電話が提供するログイン情報の有効性を確認するために、Unified Communications Manager は [エンドユーザの設定 (End User Configuration)] ウィンドウでの設定に基づいて、エンドユーザのダイジェストログイン情報を使用します。

電話が Extension Mobility をサポートする場合、Extension Mobility ユーザがログインすると、Unified Communications Manager は、[エンドユーザの設定 (End User Configuration)] ウィンドウでの設定に基づいて、Extension Mobility エンドユーザのダイジェストログイン情報を使用します。

SIP 電話機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、デバイスには一意のダイジェストユーザ ID とパスワードを登録する必要があります。電話ユーザやアプリケーションユーザには、Unified Communications Manager データベースで SIP ダイジェストログイン情報を設定する必要があります。

次の手順を実行してください。

- アプリケーションには、[アプリケーションユーザの設定 (Application User Configuration)] ウィンドウでダイジェストログイン情報を指定します。
- SIP を実行している電話には、[エンドユーザの設定 (End User Configuration)] ウィンドウでダイジェスト認証用のログイン情報を指定します。

ユーザを設定した後にログイン情報を電話と関連付けるには、[電話の設定 (Phone Configuration)] ウィンドウで[ダイジェストユーザ (Digest User)] を選択します。電話をリセットした後、ログイン情報は TFTP サーバから電話機に提供される電話設定ファイル内に存在します。

- SIP トランクで受信したチャレンジの場合、レルムユーザ名 (デバイスまたはアプリケーションユーザ) およびダイジェストログイン情報を指定する SIP レルムを設定します。



(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

SIP 電話のダイジェスト認証を設定するには、次のタスクを完了します。

手順

| | コマンドまたはアクション | 目的 |
|--------|------------------------------|--|
| ステップ 1 | 電話ユーザへのダイジェストクレデンシャルの割り当て | ダイジェストログイン情報を、電話機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のダイジェスト認証の有効化 | 電話機に関連付ける電話機の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 | 電話機へのダイジェスト認証の割り当て | [電話の設定 (Phone Configuration)] 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ます。 |
| ステップ 4 | エンドユーザのダイジェストクレデンシャルの設定 | エンドユーザダイジェストのログイン情報を設定します。 |
| ステップ 5 | SIP ステーションレルムの設定 (182 ページ) | Unified CM が Unauthorized メッセージが原因で SIP 要求をチャレンジするのに使用する [レルム (Realm)] フィールドに文字列を割り当てます。 |

電話ユーザへのダイジェストクレデンシャルの割り当て

この手順を使用して、電話を所有しているエンドユーザにダイジェストログイン情報を割り当てます。電話機は、ログイン情報を使用して認証します。

ステップ 1 Cisco Unified Communications Manager Administration で、[ユーザ管理 (User Management)] > [エンドユーザ (End User)] を選択します。

ステップ 2 [検索 (Find)] をクリックして、電話を所有しているエンドユーザを選択します。

ステップ3 次のフィールドにクレデンシャルを入力します。

- ダイジェスト クレデンシャル (Digest Credentials)
- [ダイジェストクレデンシャルの確認 (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のダイジェスト認証の有効化

電話セキュリティプロファイルを使用して電話のダイジェスト認証を有効にするには、次の手順を実行します。

ステップ1 [Cisco Unified CM の管理 (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 (Find)]をクリックして、対象の電話機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。

電話機へのダイジェスト認証の割り当て

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に対応したセキュリティプロファイルを電話機に関連付けます。

ステップ1 Cisco Unified Communications Manager Administration から、[デバイス (Device)]>[電話 (Phone)]を選択します。

ステップ2 [検索 (Find)]をクリックして、ダイジェスト認証を割り当てる電話を選択します。

ステップ3 [ダイジェストユーザ (Digest User)] ドロップダウンリストから、ダイジェストクレデンシャルを割り当てたエンドユーザを割り当てます。

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 (Device Security profile)] 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ます。

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機に関連付けた後、設定を保存し、電話機をリセットします。

SIP ステーションレームの設定

401の不正なメッセージへの応答で SIP 電話がチャレンジされた場合に、Cisco Unified Communications Manager が使用する文字列を [レーム (Realm)] フィールドに割り当てます。これは、電話機がダイジェスト認証用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。

- ステップ 1 Unified Communications Managerから、[System (システム)] > [Service Parameters (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、CiscoCallManager サービスをアクティブ化したノードを選択します。
- ステップ 3 [サービス (Service)] ドロップダウンリストから、CiscoCallManager サービスを選択します。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 ヘルプの説明に従って、SIP Realm Station パラメータを更新します。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。

エンドユーザのダイジェストクレデンシャルの設定

ダイジェストログイン情報の詳細を表示するには、次の手順を実行します。

Cisco Unified Communications Manager の管理ページから、[ユーザ管理 (User Management)] > [エンドユーザ (End User)] を選択し、[ユーザ ID (User ID)] をクリックすると、[エンドユーザの設定 (End User Configuration)] ウィンドウが表示されます。ダイジェストクレデンシャルは、[エンドユーザの設定 (End User Configuration)] ウィンドウの [ユーザ情報 (user Information)] ペインで使用できます。

表 28: ダイジェストクレデンシャル (Digest Credentials)

| 設定 | 説明 |
|---|--|
| ダイジェストクレデンシャル (Digest Credentials) | 英数字の文字列を入力します。 |
| [ダイジェストクレデンシャルの確認 (Confirm Digest Credentials)] | [ダイジェストクレデンシャル (Digest Credentials)] の入力正しいことを確認するために、このフィールドに再度クレデンシャルを入力します。 |



第 12 章

セキュアな会議リソースの設定

この章では、セキュアな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 \(183 ページ\)](#)
- [会議ブリッジの要件 \(184 ページ\)](#)
- [セキュアな会議アイコン \(185 ページ\)](#)
- [セキュアな会議のステータス \(186 ページ\)](#)
- [Cisco Unified IP 電話 セキュアな会議とアイコンのサポート \(189 ページ\)](#)
- [セキュアな会議の CTI サポート \(190 ページ\)](#)
- [トランクとゲートウェイを介したセキュアな会議 \(190 ページ\)](#)
- [CDR データ \(190 ページ\)](#)
- [連携動作と制限事項 \(190 ページ\)](#)
- [会議リソースの保護のヒント \(192 ページ\)](#)
- [セキュアな会議ブリッジのセットアップ \(194 ページ\)](#)
- [Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定 \(195 ページ\)](#)
- [ミーティングの最小セキュリティレベルの設定 \(196 ページ\)](#)
- [セキュアな会議ブリッジの packets キャプチャの設定 \(196 ページ\)](#)

セキュアな会議

セキュアな会議機能は、会議を保護するために認証と暗号化を提供します。会議は、すべての参加デバイスが暗号化されたシグナリングとメディアを持っている場合、セキュアと見なされます。セキュアな会議機能は、セキュアな TLS または IPSec 接続を介した SRTP 暗号化をサポートします。

システムには、会議の全体的なセキュリティステータスを示すセキュリティアイコンが表示されます。これは、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ます。たとえば、2つの暗号化接続と1つの認証済み接続を含むセキュアな会議には、認証済みの会議セキュリティステータスがあります。

セキュアなアドホック会議と会議室の会議を設定するには、セキュアな会議ブリッジを設定します。

- ユーザが認証済みまたは暗号化済みの電話から電話会議を開始すると、Unified Communications Manager は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な電話からコールを開始すると、Unified Communications Manager は非セキュアな会議ブリッジを割り当てます。

会議ブリッジリソースを非セキュアとして設定すると、電話のセキュリティ設定にかかわらず、会議は非セキュアになります。



- (注) Unified Communications Manager は会議を開始している電話のメディアリソースグループリスト (MRGL) から会議ブリッジを割り当てます。セキュアな会議ブリッジを使用できない場合は、Unified Communications Manager は非セキュアな会議ブリッジを割り当て、会議は非セキュアになります。同様に、非セキュアな会議ブリッジを使用できない場合、Unified Communications Manager はセキュアな会議ブリッジを割り当て、会議は非セキュアになります。会議ブリッジが使用できない場合、コールは失敗します。

会議コールの場合、会議を開始する電話機は、会議番号に設定されている最小のセキュリティ要件を満たしている必要があります。セキュアな会議ブリッジを使用できないか、発信者のセキュリティレベルが最小要件を満たさない場合、Unified Communications Manager は会議の試行を拒否します。

割り込みを使用する会議を保護するには、暗号化モードを使用するよう電話を設定します。デバイスが認証済みまたは暗号化済みの場合に [Barge] キーを押すと、Unified Communications Manager は割り込み相手とターゲットデバイスでの組み込みブリッジの間でセキュアな接続を確立します。システムは、割り込みコールで接続されているすべての通話者に対して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の Cisco Unified IP 電話 は暗号化済みコールに割り込めるようになりました。

会議ブリッジの要件

ハードウェアによる会議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場合、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 の処理のパフォーマンスに対する影響を考え、ソフトウェアによる会議ブリッジでのセキュアな会議はサポートしていません。

H.323 または MGCP ゲートウェイでの会議を実現するデジタル シグナル プロセッサ (DSP) ファームが、IP テレフォニー会議のネットワーク リソースとして動作します。会議ブリッジは、Unified Communications Manager にセキュアな SCCP クライアントとして登録されます。

- 会議ブリッジのルート証明書が CallManager 信頼ストア内に存在し、Cisco CallManager 証明書が会議ブリッジの信頼ストアに存在する必要があります。
- セキュアな会議ブリッジのセキュリティ設定は、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。

会議ルータの詳細については、IOS ルータに付属するドキュメンテーションを参照してください。

Unified Communications Manager は、コールに対して会議リソースを動的に割り当てます。使用可能な会議リソースと有効なコーデックは、ルータごとに許可される同時のセキュアな会議の最大数を提供します。送信ストリームと受信ストリームは、参加している各エンドポイントに個別にキーが割り当てられるため (参加者が会議を退室したときにキー再生成は必要ありません)、DSP モジュールの合計セキュア会議容量は、非セキュアな容量の1分に相当します。を設定できます。

『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

セキュアな会議アイコン

Cisco IP 電話 は会議全体のセキュリティ レベルを示す会議セキュリティ アイコンを表示します。これらのアイコンは、電話機のユーザマニュアルで説明されているように、セキュアな2者間コールのステータスアイコンと一致します。

コールの音声およびビデオ部分によって、会議のセキュリティレベルの基準が提供されます。音声とビデオの両方の部分がセキュアである場合にのみ、コールはセキュアと見なされます。

アドホックおよび会議のセキュアな会議では、会議の参加者の電話ウィンドウの会議ソフトウェアの横に、会議のセキュリティアイコンが表示されます。表示されるアイコンは、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、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、会議のすべての参加者が認証されている場合は、シールドアイコンが表示されます。一部の電話機モデルでは、シールドアイコンが表示されません。
- 会議ブリッジまたは会議のいずれかの参加者が非セキュアである場合、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。または、一部の古い電話機モデルでは、アイコンが表示されません。



- (注) 「コールセキュリティステータスを指定した場合の BFCP アプリケーション暗号化ステータスのオーバーライド」サービスパラメータは、パラメータ値が **True** で音声がセキュアである場合にロックアイコンを表示します。この状態は、他のすべてのメディアチャネルのセキュリティステータスを無視します。デフォルトパラメータ値は **[False]** です。

暗号化された電話機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の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応じて、暗号化、認証、または非セキュアにすることができます。非セキュアステータスは、いずれかの当事者がセキュアでないか、または検証できないことを示します。

ユーザが [割り込み (割り込み)] を押すと、[割り込み (割り込み)] ソフトキーの横に表示されるアイコンによって割り込み会議のセキュリティレベルが提供されます。割り込みデバイスと割り込まれた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つのデバイス間でメディアを暗号化しますが、接続されている通話者のセキュリティレベルに応じて、割り込み会議のステータスは非セキュア、認証済み、または暗号化済みのいずれかになります。

セキュアな会議のステータス

会議のステータスは、参加者が会議に出入りしたときに変更できます。暗号化された会議は、認証済みまたは非セキュアな参加者がコールに接続すると、認証済みまたは非セキュアのセキュリティレベルに戻ることができます。同様に、認証済みまたは非セキュアな参加者がコールを切断した場合、ステータスはアップグレードされます。非セキュアな参加者が電話会議に接続すると、その会議は非セキュアとしてレンダリングされます。

会議の状態は、参加者が会議をチェーンするとき、チェーン会議のセキュリティステータスが変更されたとき、別のデバイスで保留中の会議コールが再開されたとき、会議コールが割り込まれたとき、または転送されたときに変更することもできます。会議コールは別のデバイスに対して完了します。



- (注) Advanced Ad Hoc 会議が有効になっているサービスパラメータは、会議、参加、直接転送、転送などの機能を使用してアドホック会議をリンクできるかどうかを決定します。

Unified Communications Manager はセキュアな会議を維持するために以下のオプションを提供します。

- アドホック会議のリスト
- 最小セキュリティレベルの会議の開催

アドホック会議のリスト

会議コール中に **ConfList** ソフトキーを押すと、参加している電話機に会議リストが表示されます。会議のリストには、会議のステータスと各参加者のセキュリティステータスが表示され、暗号化されていない参加者を識別します。

会議リストには、非セキュア、認証済み、暗号化済み、保留中のセキュリティアイコンが表示されます。会議の開始者は、会議リストを使用して、セキュリティステータスが低い参加者を退出させることができます。



- (注) 高度なアドホック会議の有効化サービスパラメータは、会議の開催者以外の会議参加者が会議参加者を追放できるかどうかを決定します。

参加者が会議に参加すると、会議リストの先頭に追加されます。**ConfList** および **RmLstC** ソフトキーを使用してセキュアな会議から非セキュアな参加者を削除するには、お使いの電話機のユーザマニュアルを参照してください。

ここでは、他の機能とのセキュアなアドホック会議の相互作用について説明します。

セキュアなアドホック会議と会議チェーン

ある1つのアドホック会議が別のアドホック会議にチェーンされると、そのチェーンされた会議は、メンバー「Conference」としてそれ自体のセキュリティステータスとともにリストに表示されます。会議全体のセキュリティステータスを判別するために、**Unified Communications Manager** に、チェーンされた会議のセキュリティレベルが組み込まれます。

セキュアなアドホック会議と C 割り込み

ユーザが **[cBarge]** ソフトキーを押してアクティブな会議に参加すると、**Unified Communications Manager** ではアドホック会議が作成され、割り込まれたデバイスのセキュリティレベルと MRGL に従って会議ブリッジが割り当てられます。C 割り込みメンバー名が会議リストに表示されません。

セキュアなアドホック会議と割り込み

セキュアなアドホック会議の参加者が割り込まれた場合は、割り込みターゲットの横にある会議リスト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。割り込みの発信者には認証済みの接続があるため、割り込みターゲットと会議ブリッジの間でメディアが暗号化されている場合、割り込みターゲットのセキュリティアイコンが認証済みと表示されることがあります。

割り込みターゲットがセキュアだが非セキュアなアドホック会議では、アドホック会議のステータスが **[セキュア (secure)]** に変わると、**[割り込み発信者 (割り込み caller)]** アイコンも更新されます。

セキュアなアドホック会議と参加

認証済みまたは暗号化済みの電話ユーザは、Cisco Unified IP 電話 (sccp を実行している電話機のみ) で [参加 (Join)] ソフトキーを使用して、セキュアなアドホック会議を作成または参加できます。ユーザが [Join] を押してセキュリティステータスの不明な参加者を既存の会議に追加すると、Unified Communications Manager ではその会議のステータスを [unknown] にダウングレードします。参加している新しいメンバーを追加した参加者は会議の開催者になり、会議リストから新しいメンバーまたは他の参加者を取り出します (高度なアドホック会議が有効になっている設定が True の場合)。

セキュアなアドホック会議と保留/復帰

会議の開催者が参加者を追加するために会議コールを保留にすると、追加された参加者がコールに応答するまで、会議のステータスは [不明 (unknown)] (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、会議リストの会議ステータスが更新されます。

共有回線の発信者が別の電話で開催中の会議コールを再開すると、発信者が [再開 (Resume)] を押すと会議リストが更新されます。

最小セキュリティレベルの会議の開催

管理者は、ミーティングのパターンまたは番号を非セキュア、認証済み、または暗号化済みとして設定するときに、会議の最小セキュリティレベルを指定できます。参加者は最小のセキュリティ要件を満たしている必要があります。または、システムが参加者をブロックし、コールをドロップします。このアクションは、会議コールの転送、共有回線での会議コールの再開、およびチェーン会議に適用されます。

会議室の会議を開始する電話機が最小セキュリティレベルを満たしている必要があります。一致しない場合、システムはその試行を拒否します。最小セキュリティレベルで認証済みまたは暗号化済みが指定されていて、セキュアな会議ブリッジが使用できない場合、コールは失敗します。

会議ブリッジの最小レベルとして非セキュアを指定した場合、会議ブリッジはすべてのコールを受け入れ、会議のステータスは非セキュアになります。

ここでは、他の機能とのセキュアな会議の連携動作について説明します。

会議とアドホック会議

会議をアドホック会議に追加したり、会議にアドホック会議を追加したりするには、アドホック会議が会議の最小セキュリティレベルを満たしている必要があります。または、コールがドロップされます。会議アイコンは、会議が追加されたときに変更されることがあります。

ミーミー会議と割り込み

発信者が会議参加者を割り込むときに、割り込みの発信者が最小のセキュリティ要件を満たしていない限り、割り込まれたデバイスのセキュリティレベルがダウングレードし、割り込みの発信者と割り込まれたコールの両方がドロップされます。

会議の開催と保留/再開

電話機が最小セキュリティレベルを満たしていない限り、共有回線上の電話機が会議の開催を再開することはできません。電話機が最小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 (Resume)] 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 電話 セキュアな会議とアイコンのサポート

これらのCisco Unified IP 電話はセキュアな会議とセキュアな会議のアイコンをサポートしています。

- Cisco Unified IP 電話 7942 および 7962 (SCCP のみ、認証済みセキュア会議のみ)
- Cisco Unified IP 電話 6901、6911、6921、6941、6945、6961、7906G、7911G、7921G、7931G、7942、7941G、7941G-GE、7942G、7945G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、7975G、8941、8945。(SCCP のみ)
- Cisco Unified IP 電話 6901、6911、6921、6941、6945、6961、7906G、7911G、7941G、7941G-GE、7942G、7961G、7961G-GE、7962G、7965G、7970G、7971G、7971G-GE、7975G、8941、8945、8961、9971、9971。

Cisco IP 電話 7811、7821、7841、7861、Cisco IP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、統一 IP 会議電話機 8831、Cisco IP 会議電話 8832。



警告

セキュア会議機能を十分に活用するため、Cisco Unified IP 電話 をリリース 8.3 以降にアップグレードすることを推奨します。このリリースでは、暗号化機能がサポートされています。以前のリリースを実行している暗号化された電話は、これらの新機能を完全にはサポートしていません。そのような電話は、認証済みまたは非セキュアな参加者としてのみセキュア会議に参加できます。

リリース 8.3 の Cisco Unified IP 電話 で、以前のリリースの Cisco Unified Communications Manager が使用されている場合、電話会議の間、会議のセキュリティステータスではなく接続のセキュリティステータスが表示され、会議リストなどのセキュア会議機能もサポートされません。

Cisco Unified IP 電話 に適用されるその他の制限については、Unified Communications Manager のセキュア会議の制限関連項目を参照してください。

セキュア電話会議とセキュリティアイコンの詳細については、ご使用の電話のCisco IP 電話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。

セキュアな会議の CTI サポート

Unified Communications Manager はライセンス済み CTI デバイスでのセキュアな会議をサポートしています。詳細については、このリリースの『*Unified Communications Manager JTAPI Developers Guide*』および『*Unified Communications Manager TAPI Developers Guide*』を参照してください。

トランクとゲートウェイを介したセキュアな会議

Unified Communications Manager はクラスタ間トランク（ICT）、H.323 トランク/ゲートウェイ、および MGCP ゲートウェイを介したセキュアな会議をサポートしています。ただし、リリース 8.2 以前を実行する暗号化された電話は ICT および H.323 コールの場合 RTP に戻り、メディアは暗号化されません。

会議に SIP トランクが含まれている場合、セキュアな会議のステータス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、オフクラスタ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、電話機のエンドポイントから会議ブリッジへの各コールレグのセキュリティステータス、および会議自体のセキュリティステータスを提供します。2 つの値が CDR データベースの内の 2 つの異なるフィールドを使用します。

ミーティング会議において最も低いセキュリティレベル要件を満たさない加入の試みが拒否される場合、CDR データは終了原因コード 58 を示します（現在ベアラ機能を使用できません）。詳細については、『*CDR Analysis and Reporting Administration Guide*』を参照してください。

連携動作と制限事項

この項では、次のトピックについて説明します。

- [Cisco Unified Communications Manager のセキュアな会議とのインタラクション](#)（191 ページ）
- [セキュアな会議による Cisco Unified Communications Manager の制約事項](#)（192 ページ）

Cisco Unified Communications Manager のセキュアな会議とのインタラクション

このセクションでは、Unified Communications Manager とセキュア会議機能との間のインタラクションについて説明します。

- 会議を安全に保つために、セキュアなアドホック会議の参加者がコールを保留にするか、コールをパークする場合、[MOH を会議ブリッジに抑制 (hold MOH to call 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。セキュアな会議のステータスは変更されません。
- クラスタ間環境では、セキュアなアドホック会議でクラスタ外の会議参加者が保留を押しした場合、デバイスへのメディアストリームが停止し、MOH が再生され、メディアステータスが **unknown** に変わります。クラスタ外の参加者が MOH を使用して保留中のコールを再開すると、会議のステータスがアップグレードされることがあります。
- クラスタ間トランク (ICT) を介したセキュアな MeetMe コールは、リモートユーザが保留/再開などの電話機能を起動し、メディアステータスが **unknown** に変更されたかどうかをクリアします。
- セキュアなアドホック会議の間に参加者の電話で再生される Unified Communications Manager のマルチレベル優先度およびプリエンプションの告知トーンや告知は、会議ステータスを非セキュアに変更します。
- 発信者がセキュアな SCCP 電話コールに割り込む場合、システムはターゲットデバイスで内部トーン再生メカニズムを使用し、会議ステータスはセキュアのままになります。
- 発信者がセキュアな SIP 電話コールに割り込む場合、システムは保留トーンを再生し、トーン再生中の会議ステータスは非セキュアのままになります。
- 会議がセキュアで、RSVP が有効になっている場合、会議はセキュアのままになります。
- PSTN を含む電話会議の場合、セキュリティ会議アイコンには、コールの IP ドメイン部分のみのセキュリティステータスが表示されます。
- Maximum Call Duration Timer サービスパラメータは、会議の最大継続時間も制御します。
- 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。メディアストリームが暗号化されている場合でも、パケットキャプチャセッション中に、電話機には会議の非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って、セキュアな会議の動作が変更されることがあります。たとえば、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している場合でも、エンドポイントはシステム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。

セキュアな会議による Cisco Unified Communications Manager の制約事項

このセクションでは、セキュア会議機能に関する Unified Communications Manager の制限事項について説明します。

- 暗号化された Cisco IP 電話 でリリース 8.2 以前が実行されている場合、セキュア会議には認証済みまたは非セキュア参加者としてのみ参加できます。
- リリース 8.3 の Cisco Unified IP 電話 で、以前のリリースの Unified Communications Manager が使用されている場合、電話会議の間、会議のセキュリティステータスではなく接続のセキュリティステータスが表示され、会議リストなどのセキュア会議機能もサポートされません。
- Cisco Unified IP 電話 7800 および 7911G では、会議リストがサポートされません。
- 帯域幅の要件のため、Cisco Unified IP 電話 7942 と 7962 は、アクティブな暗号化されたコールでの暗号化されたデバイスからの割り込みをサポートしません。割り込みの試行は失敗します。
- Cisco Unified IP 電話の 79 31g は、会議のチェーンをサポートしていません。
- SIP トランクを介してコールしている電話は、デバイスのセキュリティステータスに関係なく、非セキュアな電話機として扱われます。
- セキュアな電話機が SIP トランクを介してセキュアな会議に参加しようとする、コールはドロップされます。SIP トランクでは SIP を実行中の電話に対する「device not authorized」メッセージの提供がサポートされていないため、電話がこのメッセージで更新されることはありません。さらに、SIP を実行中の 7962G 電話では、「device not authorized」メッセージがサポートされません。
- クラスタ間環境では、クラスタ外の参加者の会議リストは表示されません。ただし、クラスタ間の接続でサポートされていれば、接続のセキュリティステータスが会議ソフトキーの横に表示されます。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 (システムは認証された接続を非セキュアとして扱う) が、暗号化された接続の暗号化アイコンが表示されます。

クラスタ外の参加者は、クラスタ境界を越えて別のクラスタに接続する独自の会議を作成できます。システムは、接続された会議を基本的な2者間コールとして扱います。

会議リソースの保護のヒント

セキュアな会議ブリッジリソースを設定する前に、次の情報を考慮してください。

- セキュアな会議メッセージのカスタムテキストを電話機で表示する場合は、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 のローケルインストールのマニュアルを参照してください。

- 会議または組み込みブリッジは、会議コールを保護するために暗号化をサポートする必要があります。
- セキュアな会議ブリッジの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。
- セキュアな会議ブリッジを調達するために、会議を開始する電話機が認証または暗号化されていることを確認します。
- 共有回線で会議の整合性を維持するには、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、認証済みまたは非セキュアな電話機を使用して回線を共有するように暗号化された電話機を設定しないでください。
- クラスタ間で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 ICTs 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 ファームで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済み）は [Unified Communications Manager Administration] での会議ブリッジセキュリティモードに一致する必要があります。そうでないと、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が暗号化済みと指定されていれば、会議ブリッジは暗号化済みとして登録されます。両方のセキュリティモードが非セキュアと指定されていれば、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た場合で、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済み、会議ブリッジのセキュリティレベルが非セキュアという場合は、Unified Communications Manager は会議ブリッジ登録を拒否します。
- クラスタセキュリティモードを非セキュアモードに設定する場合、DSP ファームのセキュリティモードを非セキュアとして設定します。これにより会議ブリッジを登録できません。Unified Communications Manager Administration の設定が暗号化済みとして指定されていても、会議ブリッジは非セキュアとして登録します。
- 登録時に、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 ファームシステムに 1 つ以上の Unified Communications Manager の CallManager.pem 証明書が含まれ、Unified Communications Manager の CallManager の信頼性ストアに 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。X.509 Subject 属性で指定された共通名は、Cisco Unified Communications Manager で定義された会議ブリッジ名から開始し、関連付けプロファイル <プロファイル識別子> **register <device Name>?** コマンドを使用して DSP ファームシステムで指定する必要があります。サブジェクト代替名属性はサポートされていません。たとえば、証明書サブジェクトの共通名が ?CN=example.cisco.com? の場合、Unified Communications Manager の会議ブリッジ名は ?example? で、DSP ファームシステム コマンドは **?associate profile <profile-identifier> register example** である必要があります。同じ DSP ファームシステム上に複数のセキュアな会議ブリッジがある場合、それぞれに個別の証明書が必要です。



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構成できないことを確認してください。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。

- 会議ブリッジの証明書が何らかの理由で期限切れまたは変更された場合は、Cisco Unified Communications Operating System Administration の証明書の管理機能を使用して信頼ストアの証明書を更新します。証明書が一致しないと TLS 認証が失敗し、また会議ブリッジが動作しません。これは、会議ブリッジが Unified Communications Manager に登録できないためです。
- セキュアな会議ブリッジは、ポート 2443 で TLS 接続を介して Unified Communications Manager に登録されます。非セキュアな会議ブリッジは、ポート 2000 で TCP 接続を介して Unified Communications Manager に登録されます。
- 会議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 デバイスのリセットと Cisco CallManager サービスの再起動が必要です。

セキュアな会議ブリッジのセットアップ

次の手順では、ネットワークにセキュアな会議を追加するために使用するタスクについて説明します。

ステップ 1 CiscoCTL クライアントが混合モードにインストールされ、設定されていることを確認します。

ステップ 2 信頼ストアへの Unified Communications Manager 証明書の追加も含め、Unified Communications Manager 接続用の DSP ファームセキュリティを設定したことを確認します。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。

会議ブリッジのマニュアルを参照してください。

ヒント DSP ファームは、ポート 2443 で Unified Communications Manager への TLS ポート接続を確立します。

ステップ 3 DSP ファーム証明書が CallManager 信頼ストア内にあることを確認してください。

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 内の信頼ストアにコピーします。

証明書のコピーが終わったら、サーバで 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 Administration Guide』を参照してください。

ヒント 証明書はクラスタ内の各サーバに必ずコピーし、クラスタ内の各サーバで CiscoCallManager サービスを再起動する必要があります。

- ステップ 4** Unified Communications Manager の管理ページで、Cisco IOS Enhanced Conference Bridge を会議ブリッジタイプとして設定し、暗号化済み会議ブリッジをデバイスのセキュリティ モードとして選択します。
- ヒント 今回のリリースにアップグレードすると、Unified Communications Manager は自動的に非セキュアな会議ブリッジセキュリティプロファイルを Cisco IOS Enhanced Conference Bridge 設定に割り当てます。
- ステップ 5** ミートミー会議の最小セキュリティ レベルを設定します。
- ヒント 今回のリリースにアップグレードすると、Unified Communications Manager は最小セキュリティ レベルとして非セキュアをすべてのミートミー パターンに自動的に割り当てます。
- ステップ 6** セキュアな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、『*Troubleshooting Guide for Unified Communications Manager*』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、階層を SRTP にキャプチャします。

Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定

[Unified Communications Manager Administration] でセキュアな会議ブリッジを設定するには、次の手順を実行します。会議ブリッジに暗号化を設定した後、Unified Communications Manager の各デバイスをリセットして、Cisco CallManager 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で保護するために、Unified Communications Manager と DSP ファームにそれぞれ証明書をインストールしたことを確認してください。

始める前に

はじめる前に

- ステップ 1** [Media Resources] > [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 会議ブリッジがインストールされていることを確認し、「[セキュアな会議ブリッジのセットアップ \(194 ページ\)](#)」に進みます。
- ステップ 3** デバイスがデータベースに存在しない場合は、[新規追加 (Add New)] をクリックします。「[Cisco Unified Communications Manager Administration でのセキュアな会議ブリッジの設定 \(195 ページ\)](#)」に進みます。
- ステップ 4** [Conference Bridge Configuration] ウィンドウで、[Conference Bridge Type] ドロップダウン リストボックスから [Cisco IOS Enhanced Conference Bridge] 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、会議ブリッジの名前、説明、デバイスプール、共通デバイス設定、およびロケーション設定を構成します。
- ステップ 5** [Device Security Mode] フィールドで、[Encrypted 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

その他の会議ブリッジ設定タスクを実行するために、[Related Links] 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て [Go] をクリックし、[Meet-Me Number/Pattern Configuration] ウィンドウまたは [Service Parameter Configuration] ウィンドウに移動できます。

ミートミー会議の最小セキュリティレベルの設定

ミートミー会議の最小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。

ステップ1 [Call Routing] > [Meet-Me Number/Pattern] を選択します。

ステップ2 [会議ブリッジの検索/一覧表示 (Find and List bridge bridge)] ウィンドウで、会議番号/パターンが設定されていることを確認し、「[セキュアな会議ブリッジのセットアップ \(194 ページ\)](#)」に進みます。

ステップ3 Meet a の番号/パターンが設定されていない場合は、[新規追加 (Add New)] をクリックします。「[ミートミー会議の最小セキュリティレベルの設定 \(196 ページ\)](#)」に進みます。

ステップ4 [Meet-Me Number Configuration] ウィンドウで、[Directory Number or Pattern] フィールドにミートミー番号または範囲を入力します。『*Feature Configuration Guide for Cisco Unified Communications Manager*』の説明に従って、説明とパーティションの設定を行います。

ステップ5 [Minimum Security Level] フィールドで、[Non Secure]、[Authenticated]、または [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。

セキュアな会議ブリッジの packets キャプチャの設定

セキュアな会議ブリッジの packets キャプチャを設定するには、[サービスパラメータ設定 (Service Parameter Configuration)] ウィンドウで packets キャプチャを有効にします。次に、[デバイス設定 (device configuration)] ウィンドウで、packets キャプチャモードを batch モードに設定し、電話、ゲートウェイ、またはトランクの SRTP に階層をキャプチャします。詳細については、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

メディア ストリームが暗号化されている場合でも、パケット キャプチャ セッション中に、電話には会議について非セキュアのステータスが表示されます。



第 13 章

ボイス メッセージング ポートのセキュリティ設定

この章では、ボイスメッセージングポートのセキュリティ設定について説明します。

- [ボイスメッセージングセキュリティ \(199 ページ\)](#)
- [ボイスメッセージングセキュリティの設定のヒント \(200 ページ\)](#)
- [セキュアなボイスメッセージングポートのセットアップ \(201 ページ\)](#)
- [単一のボイスメッセージングポートへのセキュリティプロファイルの適用 \(202 ページ\)](#)
- [ボイスメールポートウィザードを使用したセキュリティプロファイルの適用 \(202 ページ\)](#)

ボイスメッセージングセキュリティ

Unified Communications Manager ボイス メッセージング ポートおよび 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 デバイスで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 ポートを選択すると TLS 接続が開始され、相互証明書交換を使用してデバイスが認証されます（各デバイスが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 ポートを選択すると、システムはまずデバイスを認証し、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 2.0 以降では、TLS ポート経由で Unified Communications Manager に接続します。デバイスセキュリティモードが非セキュアになると、Cisco Unity Connection は、SCCP ポート経由で Unified Communications Manager に接続します。



(注) この章で使用されている用語「サーバ」は、Unified Communications Manager サーバを示します。「ボイス メールサーバ」は Cisco Unity サーバまたは Cisco Unity Connection サーバを示します。

ボイスメッセージングセキュリティの設定のヒント

セキュリティを設定する前に、次の情報を考慮してください。

- Cisco Unity では、Cisco Unity Telephony Integration Manager (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 では、Cisco Unity Connection Administration 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については、Cisco Unity 向け、または Cisco Unity Connection 向けの『Unified Communications Manager integration guide』を参照してください。
- Cisco Unity 証明書を信頼ストアに保存するには、この章で説明している手順に加え、Unified Communications Manager の証明書の管理機能を使用する必要があります。

詳細については、以下の URL にある『Cisco Unified Communications Manager SCCP Integration Guide for Cisco Unity Connection』の「To Add Voice Messaging Ports in Cisco Unity Connection Administration」の手順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/cucintucmskinny230.html

証明書をコピーした後、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 証明書が期限切れになったか、何らかの理由で変更された場合は、『Cisco Unified Communications Manager アドミニストレーションガイド』の証明書の管理機能を使用して信頼ストアの証明書を更新します。証明書が一致しないと TLS 認証が失敗し、ボイスメッセージングが機能しません。これは、ボイスメッセージング機能が Unified Communications Manager に登録できないためです。
- ボイスメールサーバのポートを設定するときには、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 Telephony Integration Manager (UTIM) または Cisco Unity Connection Administration で指定する設定は、Unified Communications Manager Administration で設定されているボイスメッセージングポートのデバイスセキュリティモードと一致する必要があります。Cisco Unity Connection Administration の [Voice Mail Port Configuration] ウィンドウ（または [Voice Mail Port] ウィザード）で、ボイスメッセージング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 デバイスセキュリティモードの設定が一致しないと、Unified Communications Manager でのボイスメールサーバポートの登録は失敗し、ボイスメールサーバは登録が失敗したポートへのコールに対応できません。

- 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 デバイスのリセットとボイスメールサーバソフトウェアの再起動が必要です。Unified Communications Manager Administration で以前と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には、ボイスメールサーバの設定を変更する必要があります。

- [VoiceMail Port] ウィザードで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と、現在プロファイルに設定されているデバイスセキュリティモードは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ングポートのセットアップ

次の手順では、ボイスメッセージングポートのセキュリティを設定するために使用するタスクについて説明します。

-
- ステップ 1** `utils ctl` CLI コマンドを実行して、Unified Communications Manager が混合モードであることを確認します。
- ステップ 2** 電話機が認証または暗号化用に設定されていることを確認します。
- 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 サーバの信頼ストアにコピーし、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 Administration Guide*』を参照してください。
- (注) 以下のヒントは、リリース 14SU3 以降では無効です。
- ヒント クラスタにある各 Unified Communications Manager サーバの Cisco CTL Provider サービスをアクティブにします。次に、すべてのサーバで CiscoCallManager サービスを再起動します。
- ステップ 4** Unified Communications Manager の管理ページで、ボイスメッセージング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 のボイスメッセージングポートのセキュリティ関連設定タスクを実行します。たとえば、Cisco Unity が Cisco TFTP サーバを指すように設定します。
- 詳細については、Cisco Unity または *Cisco Unity Connection* の『*Unified Communications Manager Integration Guide*』を参照してください。
- ステップ 6** Unified Communications Manager の管理ページでデバイスをリセットし、Cisco Unity ソフトウェアを再起動します。
- 詳細については、Cisco Unity または *Cisco Unity Connection* の『*Unified Communications Manager Integration Guide*』を参照してください。
-

単一のボイスメッセージング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ング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。

この手順では、証明書がまだ存在していない場合に、デバイスをデータベースに追加し、電話機に証明書をインストールしたことを前提としています。セキュリティプロファイルを初めて適用した後、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、ボイスメッセージングセキュリティとセキュアなボイスメッセージングポートの設定に関連するトピックを確認してください。

-
- 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、ボイスメッセージングポートを検索します。
 - ステップ2 ポートの設定ウィンドウが表示されたら、[**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。データベースでは次のオプションを予め定義しています。デフォルト値は、[Not Selected] に指定されています。
 - 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たセキュリティプロファイルの適用

この手順を使用して、新しいボイスメールサーバの[ボイスメールポート (Voice Mail Port)] ウィザードで[デバイスセキュリティモード (Device Security Mode)] 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ングポートへのセキュリティプロファイルの適用に関連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、ボイスメッセージングセキュリティとセキュアなボイスメッセージングポートの設定に関連するトピックを確認してください。

-
- ステップ 1** [Unified Communications Manager Administration] で、[Voice Mail] > [Cisco Voice Mail Port Wizard] 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、[Next] 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。[Next] をクリックします。
- ステップ 4** [Cisco Voice Mail Device Information] ウィンドウで、ドロップダウンリストボックスから**デバイスセキュリティモード**を選択します。データベースでは次のオプションを予め定義しています。デフォルト値は、[Not Selected] に指定されています。
- ステップ 5** 『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、その他のデバイス設定を行います。[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、設定プロセスを続行します。[Summary] ウィンドウが表示されたら、[Finish] をクリックします。
-



第 14 章

セキュアトーンとアイコン

- [セキュアトーンとアイコンの概要 \(205 ページ\)](#)
- [セキュアアイコンとセキュアトーンのヒント \(208 ページ\)](#)
- [セキュアアイコンとセキュアトーン設定のタスク \(210 ページ\)](#)
- [セキュアコールとセキュアトーンの制限事項 \(212 ページ\)](#)

セキュアトーンとアイコンの概要

セキュアアイコンとセキュアトーンは、コールのセキュリティステータスを通知する音声および表示インジケータです。これらの機能はどちらもコールのセキュリティレベルをコールの参加者に通知するため、参加者は機密情報を安全に交換できるかどうかを理解できます。



- **セキュアアイコン**：電話機に表示されるアイコンを指し、コールのセキュリティレベルを示します。
- **セキュアトーン**：コールの開始時点で再生される2秒間のトーンを表し、コールがセキュアか非セキュアかを示します。

セキュアアイコン

セキュリティアイコンは、電話機のディスプレイに表示される視覚的なインジケータで、コールがセキュアなのか非セキュアなのかを知らせます。このアイコンは、電話機の通話時間タイマーの横に表示されます。

次の表に、セキュリティアイコンとその意味の説明を示します。

表 29: セキュアアイコン

| セキュリティアイコン | セキュリティレベル | 説明 |
|---|-----------|--|
| ロック  | 暗号化された通話 | <p>コールシグナリング (TLS を使用) とコールメディア (SRTP を使用) の両方が暗号化されます。</p> <p>(注) 暗号化アイコンが電話機に表示されるには、音声ストリームを常に暗号化する必要があります。コールセキュアステータスポリシーパラメータの設定方法に応じて、追加のメディアストリーム (ビデオ、BFCP、および iX チャネル) の暗号化が必要な場合があります。デフォルト値では、音声ストリームとビデオストリームの両方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。</p> |
| シールド  | 認証済みコール | <p>コールシグナリングは TLS で暗号化され、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ます。</p> <p>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。ただし、コールセキュアステータスポリシーは、コールが暗号化されたステータスになるには両方を暗号化する必要があるというメッセージを示しています。</p> |
| アイコンなし | 非セキュアコール | 非セキュアな音声およびビデオを備えた未認証デバイス |

追加情報

- 一部の電話機モデルでは、ロックアイコン (暗号化) のみ表示され、保護アイコン (認証済み) は表示されません。
- 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、クラスタ間、クラスタ間、およびマルチホップコールで変更できます。SCCP 回線、SIP 回線、および H.323 シグナルトーンは、参加しているエンドポイントに対するコールセキュリティステータスの変化に関する通知をサポートします。
- 電話会議と割り込みコールでは、セキュリティアイコンは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、コールの開始時点で保護された電話機で再生されるように設定できます。このトーンは、通話中の相手のデバイスがセキュアか非セキュアかを知らせます。相手方のデバイスがセキュアでない場合は、非セキュアトーンが聞こえ、相手方のデバイスがセキュアな場合は、セキュアトーンが聞こえます。

すべての電話機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た電話機でのみ再生されます。コール内の両方の電話機が保護されているが、保護される電話機が1つだけである場合、保護された電話機だけでそのトーンが聞こえます。

次の表に、トーンのタイプとそれぞれの意味を示します。

表 30: 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。他の電話機はセキュアです。 |
| 短いビープ音 6 個 | 非セキュアコール。他の電話機はセキュアではありません。 |

コール途中での変更

コール中にコールのセキュリティステータスが変った場合、新しいセキュリティステータスの保護されたデバイス上で発信者にアラートを通知するために、新しいセキュアまたは非セキュアトーンがコール途中で再生されます。保護されているデバイスを使用しているユーザにだけ、次のトーンが聞こえます。

コールのタイプ

セキュアトーンは、次のタイプのコールで機能します。

- クラスタ間のコール (IP-to-IP)
- 保護されていると見なされるクラスター間コール
- 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されている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

ユーザの電話機および相手側の電話機でセキュアなコールが設定されている場合にセキュアなコールを確立および識別できます。会議コールでは、セキュアな会議ブリッジがセットされると、セキュアなコールがサポートされるようになります。

セキュアな電話機 (セキュアモード) からコールを開始すると、セキュアなコールが確立されます。セキュアアイコンが電話機の画面に表示され、その電話機がセキュアなコール用に設定されていることが示されますが、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ているわけではありません。

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、両端の会話が暗号化されており、セキュアであることを示します。





(注) コールがセキュアでない電話機に接続されている場合、セキュリティトーンは聞こえません。

セキュアアイコンとセキュアトーンのヒント

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。保護された電話機では、セキュアなコールが設定されている場合、会議コール、共有電話、エクステンションモビリティなどの機能を使用できません。保護されている電話機の発信者にのみ、セキュア通知トーンと非セキュア通知トーンが聞こえます。保護されていない電話機の発信者には、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。

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

- 電話機には、認証のシグナリングセキュリティレベルを示す、コールの保護アイコン  が表示されます。保護アイコンは、Cisco IP デバイス間のセキュリティで保護された接続を識別します。このアイコンは、デバイスが暗号化されたシグナリングを使用していることを示します。
- 電話機に暗号化されたメディアを使用する  コールにはロックアイコンが表示されます。このアイコンは、デバイスが暗号化されたシグナリングおよび暗号化されたメディアを使用することを示します。
- 一部の電話機モデルでは、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、クラスタ間、クラスタ間、およびマルチホップコールで変更できます。SCCP回線、SIP回線、およびh.323シグナリングは、参加しているエンドポイントに対するコールセキュリティステータスの変更に関する通知をサポートします。

保護された電話機だけで、セキュアまたは非セキュア通知トーンが再生されます。保護されていない電話機では、通知トーンは再生されません。コール中にコール全体のステータスが変化すると、それに従って通知トーンも変更され、保護された電話機は対応するトーンを再生します。

保護された電話機が適切なトーンを再生するシナリオは次のとおりです。

- [セキュア通知トーンの再生 (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、電話機はセキュア通知トーン (間に小休止を伴う3回の長いビーブ音) を再生します。

- エンドツーエンドの非セキュアなメディアが確立され、コールステータスが非セキュアになった場合、電話機は、非セキュア通知トーンを再生します（間に小休止を伴う6回の短いビープ音）。
- [セキュア通知トーンの再生 (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。

サポートされるデバイスのセキュアトーン

セキュアトーンをサポートする電話機のリストを取得するには、次の手順を使用します。

- 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 (Generate a New Report)] をクリックします。
- ステップ 4 [機能 (Features)] ドロップダウンリストから、[セキュアトーン (Secure Tone)] 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。

保護されたデバイスのセキュアトーン

Unified Communications Manager で、サポートされている Cisco Unified IP Phone ゲートウェイと MGCP E1 PRI ゲートウェイのみを保護されたデバイスとして設定することができます。また、Unified Communications Manager では、システムがコールの保護されたステータスを判定するときに、セキュアおよび非セキュア通知トーンを再生するように、MGCP IOS ゲートウェイに指定することもできます。

セキュア通知トーンと非セキュア通知トーンを使用する次のタイプのコールを発信できます。

- クラスタ間の IP-to-IP コール
- システムが保護されていると判断するクラスタ間コール
- 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。

保護されたデバイスは次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接続先が暗号化されていなくても、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。

- 保護されている電話機が保護されている他の電話機に発信し、メディアが暗号化されていない場合、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。

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 [電話の設定 (Phone Configuration)] ウィンドウで、[保護されたデバイス (Protected Device)] チェックボックスをオンにします。

セキュアアイコンとセキュアトーン設定のタスク

次のタスクを使用して、セキュアアイコンとセキュアトーンを設定できます。

手順

| | コマンドまたはアクション | 目的 |
|--------|--------------------|--|
| ステップ 1 | セキュアアイコンポリシーの設定 | コールセキュアステータスポリシーでは、セキュアアイコン機能でコールを [暗号化済み (Encrypted)] と表示するために、コール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について概要を説明します。デフォルトでは、音声とビデオ (ビデオコールの場合) の両方を暗号化する必要があります。設定を再設定して、BFCP および iX チャネルも考慮できます。 |
| ステップ 2 | クラスタのセキュア通知トーンの有効化 | 保護された電話機でセキュア通知トーンを有効にします。 |
| ステップ 3 | 電話機の保護デバイスとしての設定 | Unified Communications Manager で、サポートされている Cisco Unified IP Phone を保護されているデバイスとして設定します。 |

セキュアアイコンポリシーの設定

コールセキュアステータスポリシーは、電話機のセキュアステータスアイコンの表示を制御します。ポリシーのオプションは次のとおりです。

- 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が暗号化されている必要があります。

これはデフォルト値です。コール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が暗号化されている必要があります

コールのセキュリティステータスは、暗号化ステータス iX アプリケーションストリームに依存しません。

- 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が暗号化されている必要があります

コールのセキュリティステータスは、BFCP 暗号化ステータスに依存しません。

- セッション内のすべてのメディアが暗号化されている必要があります

コール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よって異なります。

- 音声のみを暗号化する必要があります

コールのセキュリティステータスは、オーディオストリームの暗号化によって異なります。



(注) ポリシーの変更は、電話機のセキュアなアイコンの表示とセキュアトーンの再生に影響しません。

-
- 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)] を選択します。
- ステップ 2** [サーバとサービスの選択 (Select Server and Service)] ペインで、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 - コールセキュアステータスポリシー) (Clusterwide Parameters (Feature - Call Secure Status Policy))] ペインに進みます。
- ステップ 4** [セキュアコールアイコンの表示ポリシー (Secure Call Icon Display Policy)] フィールドで、ドロップダウンリスト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への影響を示す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 の [サービスパラメータの設定 (Service Parameter Configuration)] ページでポリシーが更新されます。
-

クラスタのセキュア通知トーンの有効化

セキュア通知トーンは、コールの全体的なステータスが保護されている場合、システムが、コールが暗号化されていると判断した場合に保護対象の電話で再生されます。通知トーンを True に設定する必要があります。

-
- 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)] を選択します。

- ステップ2 [サーバとサービスの選択 (Select Server and Service)] ペインで、サーバと CallManager サービスを選択します。
- ステップ3 [クラスタワイドパラメータ (機能 - セキュアトーン) (Clusterwide Parameters (Feature - Secure Tone))] ペインに移動します。
- ステップ4 [セキュア/非セキュアコールのステータスを示すトーンの再生 (Play Tone to Indicate Secure/Non-Secure Call Status)] を [True] に設定します。デフォルトでは、このオプションは [False] です。
セキュア通知トーン用にクラスタを設定した後、個々の電話機を保護された電話機として設定します。セキュアトーンと非セキュアトーンは、保護された電話機でのみ聞こえます。

電話機の保護デバイスとしての設定

Unified Communications Manager で、サポートされている Cisco Unified IP Phone を保護されたデバイスとして設定できます。保護されている電話機の発信者にのみ、セキュア通知トーンと非セキュア通知トーンが聞こえます。

- ステップ1 [Cisco Unified CM Administration] から、[デバイス (Device)] > [電話機 (Phone)] の順に選択します。電話機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 [デバイス情報 (Device Information)] ペインに移動し、次の操作を実行します。
- [ソフトキーテンプレート (Softkey Template)] ドロップダウンリストから、[標準保護電話 (Standard Protected Phone)] 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。
 - [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 [プロトコル固有の情報 (Protocol Specific Information)] ペインに移動します。
- ステップ5 [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から、[電話のセキュリティプロファイルの設定 (Phone Security Profile Configuration)] ページですでに設定されている暗号化されたセキュリティ電話機プロファイルを選択します。
- ステップ6 [保存 (Save)] をクリックします。

セキュアコールとセキュアトーンの制限事項

セキュアコールとセキュアトーンに関する制限事項を次に示します。

表 31: セキュアアイコンとセキュアトーンの連動操作と制限事項

| 機能 | 連携動作と制限事項 |
|------------|--|
| H.323 トランク | H.323 トランクでサポートされないセキュアアイコン |
| コールの転送と保留 | コールの転送や保留などのタスクを実行すると、暗号化ロックアイコンが電話機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ているメディアストリームが暗号化されていない場合、ステータスは暗号化から非セキュアに変わります。 |
| PSTN コール | PSTN を含むコールの場合、セキュリティアイコンには、コールの IP ドメイン部分のみのセキュリティステータスが表示されます。 |
| 割り込み | <p>セキュアアイコンを使用する場合：</p> <ul style="list-style-type: none"> 非セキュアまたは認証されていない Cisco IP 電話は、暗号化されたコールに割り込むことができます。[セキュリティ (security)] アイコンは、会議コールのセキュリティステータスを示します。 <p>セキュアトーンの場合：</p> <ul style="list-style-type: none"> 発信者がセキュアな SIP コールに割り込む場合、システムは保留トーンを再生し、トーンの間 Unified Communications Manager が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 コールに割り込む場合、システムはターゲットデバイスで内部トーン再生メカニズムを使用し、ステータスはセキュアのままになります。 |



第 15 章

トランクとゲートウェイの SIP セキュリティ

- [トランクとゲートウェイの SIP セキュリティの概要 \(215 ページ\)](#)
- [トランクとゲートウェイの SIP セキュリティ設定タスクフロー, on page 220](#)

トランクとゲートウェイの SIP セキュリティの概要

このセクションでは、SIP トランクの暗号化、ゲートウェイの暗号化の概要、およびセキュリティプロファイル設定のヒントについて説明します。

SIP トランクの暗号化

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 はシグナリング暗号化を提供し、SRTP はメディア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 trunk security profile)] ウィンドウで) を設定するとき、次のオプションを選択します。

- [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、「[暗号化済 (Encrypted)]」を選択します。
- [着信転送タイプ (Incoming Transport Type)] ドロップダウンリストから「[TLS]」を選択します。
- [発信転送タイプ (Outgoing Transport Type)] 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、そのプロファイルをトランクに適用します ([Device > trunk > sip trunk configuration] ウィンドウ)。

トランクに対してメディア暗号化を設定するには、[SRTPを許可 (SRTP Allowed)] チェックボックスをオンにします ([デバイス (Device)][トランク][SIP トランク (SIP Trunk)] 設定ウィンドウでも同様です)。



注意 このチェックボックスをオンにする場合は、キーやその他のセキュリティ関連情報がコールネゴシエーション中に公開されないように、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。非セキュアプロファイルを使用する場合でも SRTP は機能しますが、キーはシグナリングおよび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 ゲートウェイの暗号化

Unified Communications Manager は、MGCP SRTP パッケージを使用するゲートウェイをサポートしています。MGCP SRTP パッケージは、ゲートウェイがセキュア RTP 接続上でパケットを暗号化および復号化するとき使用されます。コールセットアップ中に交換される情報によって、ゲートウェイがコールに 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。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（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送、会議、トランスコーディング、保留音などの場合に発生する可能性があります。

システムが2台のデバイス間で暗号化 SRTP コールを設定する場合、Unified Communications Manager はセキュアコール用のマスター暗号化キーと salt を生成し、SRTP ストリーム専用のゲートウェイに送信します。Unified Communications Manager は SRTCP ストリーム用のキーと salt を送信しませんが、ゲートウェイはこれらもサポートします。これらのキーは、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。このパスは IPsec を使用して保護する必要があります。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、システムはゲートウェイにセッションキーをクリアテキストで送信します。セッションキーがセキュアな接続を介して送信されるよう、IPsec 接続が存在することを確認します。



ヒント SRTP 用に設定されている MGCP ゲートウェイが、認証済みデバイス（たとえば、SCCP を実行している認証済み電話機）とのコールに関与している場合、Unified Communications Manager がコールを認証済みとして分類するため、電話機に保護アイコンが表示されます。Unified Communications Manager は、デバイスの SRTP 機能がコールのネゴシエートに成功した場合、コールを暗号化として分類します。MGCP ゲートウェイが、セキュリティアイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話に鍵アイコンが表示されます。

次に、MGCP E1 PRI ゲートウェイについての説明を示します。

- SRTP 暗号化の MGCP ゲートウェイを設定する必要があります。コマンド **mgcppackage-capabilitysrtp-package** を使用してゲートウェイを設定します。
- MGCP ゲートウェイでは、[高度な IP サービス (Advanced IP Services)] または [高度な企業サービス (Advanced Enterprise Services)] イメージを指定する必要があります。

たとえば、**c3745-adventerprisek9-mz.124-6.T.bin** など。

- 保護ステータスは、COCP PRI Setup、Alert、および Connect の各メッセージで独自の FacilityIE を使用して、交換用の CP E1 PRI ゲートウェイと交換されます。
- Unified Communications Manager は、Cisco Unified IP 電話 でのみセキュア通知トーンを再生します。ネットワーク内の PBX は、コールのゲートウェイ側にトーンを再生します。
- Cisco Unified IP 電話 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と、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、使用している Cisco IOS ソフトウェアのバージョンの『*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.323/h トランク暗号化 (h.323)

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、または非ゲートキーパー制御の H.225/H.323/H.245 トランクは、Cisco Unified Communications Operating System で IPsec アソシエーションを設定した場合、Unified Communications Manager に対して認証できません。Unified Communications Manager とこれらのデバイスの間での IPsec アソシエーション作成については、『*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、および H.245 デバイスでは暗号キーが生成されます。これらのキーは、IPsec で保護されたシグナリング パスを介して Unified Communications Manager に送信されます。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 キーは暗号化されずに送信されます。セッション キーがセキュアな接続を介して送信されるよう、IPsec 接続が存在することを確認します。

IPsec アソシエーションの設定に加えて、Unified Communications Manager Administration のデバイス設定ウィンドウにある [SRTP 許可 (SRTP Allowed)] チェックボックスにマークを付ける必要があります。これは H.323 ゲートウェイ、H.225 トランク (ゲートキーパー制御)、クラスタ間トランク (ゲートキーパー制御)、およびクラスタ間トランク (非ゲートキーパー制御) の設定ウィンドウなどに存在します。このチェックボックスをオンにしない場合、Unified Communications Manager は RTP を使用してデバイスと通信します。このチェックボックスをオンにする場合、Unified Communications Manager は SRTP がデバイスに対して設定されているかどうかに応じて、セキュア コールと非セキュア コールを許可します。



注意 Unified Communications Manager Administration で [SRTP Allowed] チェックボックスをオンにする場合は、セキュリティ関連情報が暗号化されずに送信されることを防ぐために、IPSec を設定することを強く推奨します。

Unified Communications Manager は、IPSec 接続が正しく設定されたかどうかを確認しません。接続を正しく設定しないと、セキュリティ関連の情報がクリアテキストで送信されることがあります。

セキュアメディアパスまたはセキュアシグナリングパスを確立でき、デバイスが SRTP をサポートする場合、システムは SRTP 接続を使用します。セキュアメディアパスまたはセキュアシグナリングパスを確立できないか、1つ以上のデバイスが SRTP をサポートしない場合、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（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送、会議、トランスコーディング、保留音などの場合に発生する可能性があります。



ヒント コールがパススルー対応 MTP を使用し、リージョンフィルタリングの後でデバイスの音声機能が一致し、どのデバイスについても [MTP Required] チェックボックスがオンになっていない場合、Unified Communications Manager はそのコールをセキュアとして分類します。[MTP Required] チェックボックスがオンの場合、Unified Communications Manager はコールの音声パススルーを無効にし、コールを非セキュアとして分類します。MTP がコールに関係しない場合、Unified Communications Manager はデバイスの SRTP 機能に応じてそのコールを暗号化済みに分類することがあります。

Unified Communications Manager は、そのデバイスの [SRTP Allowed] チェックボックスがオンで、そのデバイスの SRTP 機能がコールに対して正常にネゴシエートされれば、コールを暗号化済みに分類します。コールを暗号化済みとして分類します。前述の条件を満たさない場合、Unified Communications Manager はコールを非セキュアとして分類します。デバイスが、セキュリティアイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話機に鍵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経由の発信 FastStart コールを非セキュアとして分類します。Unified Communications Manager Administration で [SRTP Allowed] チェックボックスをオンにした場合、Unified Communications Manager は [Enable Outbound FastStart] チェックボックスをオフにします。

Unified Communications Manager の一部の種類のゲートウェイおよびトランクでは、共有秘密キー（Diffie-Hellman キー）やその他の H.235 データを 2つの H.235 エンドポイント間で透過的にパススルーさせることができます。このため、これら2つのエンドポイントではセキュアメディアチャネルを確立できます。

[H. 235 data] の通過を有効にするには、次のトランクおよびゲートウェイの構成時の設定で [h. 235 パススルーを許可する] チェックボックスをオンにします。

- 「-225 Trunk」

- ICT ゲートキーパー制御
- ICT 非ゲートキーパー制御
- H.323 ゲートウェイ

トランクとゲートウェイの設定の詳細については、『*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。

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、単一のセキュリティ 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るよう、SIP トランクのセキュリティ関連の設定項目をグループ化しています。セキュリティ関連の設定項目には、デバイスセキュリティモード、ダイジェスト認証、着信/発信転送タイプの設定があります。[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する際に、構成済みの設定を SIP トランクに適用します。

Unified Communications Manager をインストールすると、自動登録用の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、それを 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ない場合は、非セキュアプロファイルを選択してください。

セキュリティプロファイルの設定ウィンドウには、SIP トランクがサポートするセキュリティ機能だけが表示されます。

SIP トランク セキュリティ プロファイルの設定のヒント

[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際に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は、非セキュアプロファイルを選択します。
- 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は削除できません。
- 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と、そのプロファイルが割り当てられているすべての SIP トランクに再設定された設定が適用されます。
- 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前提としています。
- Unified Communications Manager 5.0 以降のアップグレード前にデバイスセキュリティモードを設定していた場合、Unified Communications Manager は SIP トランクのプロファイルを作成し、その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 セキュリティ設定タスクフロー

次のタスクを実行して、ゲートウェイと SIP のセキュリティを構成します。

Procedure

| | Command or Action | Purpose |
|--------|--|--|
| ステップ 1 | セキュア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 プロファイルの設定 | 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 | トランクへの SIP トランクセキュリティプロファイルを有効にし、デバイスにセキュリティプロファイルを適用します。 |
| ステップ 4 | Sip トランクセキュリティプロファイルと SIP トランクの同期 | SIP トランクセキュリティプロファイルと SIP トランクを同期します。 |
| ステップ 5 | Cisco Unified Communications Manager Administration を使用した SRTP の許可 | H.323 ゲートウェイおよびゲートキーパー制御または非ゲートキーパー制御の 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。 |

セキュアゲートウェイとトランクのセットアップ

この手順は、CiscoIOS のメディアおよびシグナリングの認証および暗号化機能と組み合わせで使用します。これにより、セキュリティのために CiscoIOS MGCP ゲートウェイを設定する方法に関する情報が提供されます。

ステップ 1 **ctls 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ます。

ステップ 2 電話機が暗号化用に設定されていることを確認します。

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ストラクチャで IPSec を設定することも、Unified Communications Manager とゲートウェイまたはトランクとの間で IPSec を設定することもできます。IPSec を設定するために 1 つの方式を実装する場合、他の方式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、Unified Communications Manager で [SRTP を許可する (SRTP Allowed)] チェックボックスをオンにします。

[SRTPを許可する (SRTP Allowed)] チェックボックスは、[トランクの設定 (Trunk Configuration)] ウィンドウまたは[ゲートウェイの設定 (Gateway Configuration)] ウィンドウに表示されます。これらのウィンドウを表示する方法については、[Cisco Unified Communications Manager アドミニストレーションガイド](#)のトランクおよびゲートウェイに関する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（この処理を行っていない場合）。また、[デバイス (Device)] > [トランク (Trunk)] > [SIP トランク (SIP Trunk)] の設定ウィンドウで [SRTP を許可する (SRTP allowed)] チェックボックスを必ずオンにします。

注意 [SRTP を許可する (SRTP Allowed)] チェックボックスをオンにする場合、コールネゴシエーション中にキーやその他のセキュリティ関連情報が公開されないようにするために、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。非セキュアプロファイルを使用すると、SRTP は機能しますが、キーはシグナリングおよび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、『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』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

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、次の手順を実行します。

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)] > [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 次のいずれかの操作を行います。

- a) 新しいプロファイルを追加するには、[Find] ウィンドウで [Add New] をクリックします
(プロファイルを表示してから、[Add New] をクリックすることもできます)。
各フィールドにデフォルト設定が取り込まれた設定ウィンドウが表示されます。
- 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、[Copy] 列内にあるそのレコード用の [Copy] アイコンをクリックします
(プロファイルを表示してから、[Copy] をクリックすることもできます)。
設定ウィンドウが表示され、設定された項目が示されます。
- 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](#)」の説明に従い、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。
設定ウィンドウが表示され、現在の設定が示されます。

ステップ 3 「SIP トランク セキュリティ プロファイルの設定」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、それをトランクに適用します。SIP トランクにダイジェスト認証を設定した場合は、SIP トランクを介して接続されているアプリケーションの [**Sip レalm (Sip Realm)**] ウィンドウでダイジェストクレデンシャルを設定する必要があります (まだ設定していない場合)。SIP トランクを介して接続されてい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許可を有効にした場合は、[**アプリケーションユーザ (Application User)**] ウィンドウでアプリケーションに許可されているメソッドを設定する必要があります (まだ実行していない場合)。

SIP トランク セキュリティ プロファイルの設定

次の表では、[SIP トランク セキュリティ プロファイル (SIP Trunk Security Profile)] の設定項目について説明します。

表 32: 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、[トランクの設定 (Trunk Configuration)] ウィンドウの [SIP トランク セキュリティ プロファイルの設定 (SIP Trunk Security Profile)] ドロップダウンリストにその名前が表示されます。 |
| [説明 (Description)] | 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、任意の言語で最大 50 文字を指定できますが、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)] | <p>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。</p> <ul style="list-style-type: none"> • [非セキュア (Non Secure)] : イメージ認証以外のセキュリティ機能は適用されません。TCP または UDP 接続で Unified Communications Manager が利用できます。 • [認証済み (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 接続が開きます。 • [暗号化 (Encrypted)] : Unified Communications Manager はトランクの整合性、認証、およびシグナリング暗号化を提供します。AES128/SHA を使用する TLS 接続がシグナリング用に開きます。 <p>(注) [認証済み (Authenticated)]として選択されている [デバイスセキュリティプロファイル (Device Security Profile)] を使用してトランクを設定した場合、Unified Communications Manager は、NULL_SHA 暗号を使用した TLS 接続 (データ暗号化なし) を開始します。</p> <p>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。</p> <p>NULL_SHA 暗号をサポートしていない接続先デバイスでは、トランクを [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 (Device Security Profile)] オプション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。</p> |
| [Incoming Transport Type] | <p>[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、転送タイプは TCP+UDP になります。</p> <p>[デバイスセキュリティモード (Device Security Mode)] が [認証済み (Authenticated)] または [暗号化 (Encrypted)] の場合、TLS で転送タイプが指定されます。</p> <p>(注) Transport Layer Security (TLS) プロトコルによって、Unified Communications Manager とトランク間の接続が保護されます。</p> |

| 設定 | 説明 |
|--|---|
| [発信転送タイプ (Outgoing Transport Type)] | <p>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。</p> <p>[デバイスセキュリティモード (Device Security Mode)]が [非セキュア (Non Secure)]の場合は、[TCP] または [UDP] を選択します。</p> <p>[デバイスセキュリティモード (Device Security Mode)]が [認証済 (Authenticated)] または [暗号化 (Encrypted)] の場合、TLS で転送タイプが指定されます。</p> <p>(注) TLSにより、SIP トランクのシグナリング完全性、デバイス認証、およびシグナリング暗号化が保証されます。</p> <p>(注) Unified Communications Manager システム間の SIP トランクを接続し、他のアプリケーションが TCP をサポートしていない場合にのみ、発信トランスポートタイプとして UDP を使用する必要があります。それ以外の場合は、デフォルトのオプションとして TCP を使用します。</p> |
| [ダイジェスト認証の有効化 (Enable Digest Authentication)] | <p>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 要求に対してチャレンジを行います。</p> <p>ダイジェスト認証では、デバイス認証、完全性、および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 [認証済 (Authenticated)] または [暗号化 (Encrypted)] を選択してください。</p> <p>ヒント TCP または UDP 転送を使用しているトランクでの 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。</p> |
| [ナンス確認時間 (Nonce Validity Time)] | <p>ナンス値が有効な分数 (秒単位) を入力します。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。</p> <p>(注) ナンス値は、ダイジェスト認証をサポートする乱数であり、ダイジェスト認証パスワードの MD5 ハッシュを計算するときに使用されます。</p> |

| 設定 | 説明 |
|--|--|
| <p>[Secure Certificate Subject or Subject Alternate Name (安全な証明書の件名またはサブジェクトの別名)]</p> | <p>このフィールドは、着信転送タイプおよび発信転送タイプに TLS を設定した場合に適用されます。</p> <p>デバイス認証では、SIP トランク デバイスのセキュアな証明書のサブジェクトまたはサブジェクト代替名を入力します。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ことがあります。このように解決された場合、トランクに複数のセキュアな証明書のサブジェクトまたはサブジェクト代替名が設定されます。X.509 のサブジェクト名が複数存在する場合、スペース、カンマ、セミコロン、コロンのいずれかを入力して名前を区切ります。</p> <p>このフィールドには、4096 文字まで入力できます。</p> <p>ヒント サブジェクト名は、送信元接続 TLS 証明書に対応します。サブジェクト名とポートごとにサブジェクト名が一意になるようにしてください。異なる SIP トランクに同じサブジェクト名と着信ポートの組み合わせを割り当てることはできません。例: ポート 5061 の SIP TLS trunk1 は、セキュリティ保護された証明書の件名またはサブジェクト代替名 my_cm1, my_cm2 を持っています。ポート 5071 の SIP TLS trunk2 には、セキュリティで保護された証明書のサブジェクトまたはサブジェクト代替名 my_cm2, my_cm3 があります。ポート 5061 の SIP TLS trunk3 は、セキュリティで保護された証明書の件名またはサブジェクト代替名 my_ccm4 を含むことができますが、安全な証明書のサブジェクトまたはサブジェクト代替名 my_cm1 を含めることはできません。</p> |

| 設定 | 説明 |
|---|--|
| [着信ポート (Incoming Port)] | <p>着信ポートを選択します。0 ~ 65535 の範囲の一意的なポート番号値を1つ入力します。着信 TCP および UDP SIP メッセージのデフォルトポート値として 5060 が指定されます。着信 TLS メッセージのデフォルトの保護された SIP ポートには 5061 が指定されます。ここで入力した値は、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。</p> <p>ヒント TLS を使用するすべての SIP トランクは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 トランクは同じ着信ポートを共有できます。同じポートで、TLS SIP 転送トランクと TLS 以外の SIP 転送トランクタイプを混在させることはできません。</p> <p>ヒント 通常のトラフィック時に、SIP トランク UDP ポートで1つの IP アドレスからの着信パケットレートが、設定済み [SIP トランク UDP ポートのスロットルしきい値 (SIP Trunk UDP Port Throttle Threshold)] を超える場合には、しきい値を設定し直してください。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、Unified Communications Manager は2つのサービスパラメータ値の高い方に基づいてパケットをスロットリングします。このパラメータの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。</p> |
| [アプリケーションレベル認証を有効化 (Enable Application Level Authorization)] | <p>アプリケーションレベルの認証が、SIP トランクを介して接続されたアプリケーションに適用されます。</p> <p>このチェックボックスをオンにする場合、[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て、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、許可されているアプリケーション方式を確認する前に、SIP アプリケーションユーザを認証します。</p> <p>アプリケーションレベルの許可が有効な場合、トランクレベルの許可が最初に発生してからアプリケーションレベルの許可が発生するため、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対して許可されたメソッドより先に、(このセキュリティプロファイル内の) トランクに対して許可されたメソッドをチェックします。</p> <p>ヒント アプリケーションを信頼性を識別できない場合、または特定のトランクでアプリケーションが信頼されない場合 (つまり、予期したものとは異なるトランクからアプリケーション要求が着信する場合) には、アプリケーションレベル認証の使用を考慮してください。</p> |

| 設定 | 説明 |
|--|---|
| <p>[プレゼンスの SUBSCRIBE の許可 (Accept Presence Subscription)]</p> | <p>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。</p> <p>[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、この機能に関して許可され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。</p> <p>アプリケーション レベルの認証が有効な場合、[プレゼンスの SUBSCRIBE の許可 (Accept Presence Subscription)] チェックボックスがアプリケーション ユーザに関してオンに設定され、トランクに関してはオンに設定されない場合、トランクに接続される 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。</p> |
| <p>[Out-of-Dialog REFER の許可 (Accept Out-of-dialog REFER)]</p> | <p>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。</p> <p>[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、この方式に関して許可され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。</p> |
| <p>[Unsolicited NOTIFY の許可 (Accept Unsolicited Notification)]</p> | <p>Unified Communications Manager が SIP トランク経由で着信する非 INVITE、Unsolicited NOTIFY 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。</p> <p>[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、この方式に関して許可され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。</p> |

| 設定 | 説明 |
|---|--|
| [ヘッダー置き換えの許可 (Accept Replaces Header)] | <p>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。</p> <p>[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、この方式に関して許可される [ヘッダー置き換えの許可 (Accept Header Replacement)] チェックボックスをオンにします。</p> |
| [セキュリティステータスを送信 (Transmit Security Status)] | <p>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。</p> <p>デフォルトでは、このボックスはオフになっています。</p> |
| [SIP V.150アウトバウンドSDPオファ어의フィルタリング (SIP V.150 Outbound SDP Offer Filtering)] | <p>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。</p> <ul style="list-style-type: none"> • [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 アウトバウンド SDP オファ어의フィルタリング (SIP V.150 Outbound SDP Offer Filtering)] サービスパラメータで指定されたデフォルトフィルタを使用します。このサービスパラメータを見つけるには、Cisco Unified Communications Manager Administrationで、[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))] の順に移動します。 • [フィルタなし (No Filtering)] : SIP トランクは、アウトバウンドオファ어内の V.150 SDP 行のフィルタリングを実行しません。 • [MER V.150 を削除 (Remove MER V.150)] : SIP トランクは、アウトバウンドオファ어内の V.150 MER SDP 行を削除します。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。 • [Remove Pre-MER V.150] : SIP トランクは、アウトバウンドオファ어で非 MER 対応 V.150 回線をすべて削除します。クラスタがプレ MER 回線でオファ어를処理できない MER 準拠デバイスのネットワークに含まれ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。 |

| 設定 | 説明 |
|---|---|
| [SIP V.150アウトバウンドSDPオファ어의フィルタリング (SIP V.150 Outbound SDP Offer Filtering)] | <p>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。</p> <ul style="list-style-type: none"> • [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 アウトバウンド SDP オファ어의フィルタリング (SIP V.150 Outbound SDP Offer Filtering)] サービス パラメータで指定されたデフォルト フィルタを使用します。このサービスパラメータを見つけるには、Cisco Unified Communications Manager Administrationで、[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))] の順に移動します。 • [フィルタなし (No Filtering)] : SIP トランクは、アウトバウンドオファ어内の V.150 SDP 行のフィルタリングを実行しません。 • [MER V.150 を削除 (Remove MER V.150)] : SIP トランクは、アウトバウンドオファ어内の V.150 MER SDP 行を削除します。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。 • [Remove Pre-MER V.150] : SIP トランクは、アウトバウンドオファ어で非 MER 対応 V.150 回線をすべて削除します。MER より前の行を使用するオファ어를処理できない MER 準拠デバイスからなるネットワークにクラスタが含まれている場合、あいまいさを減らすには、このオプションを選択します。 <p>(注) セキュアなコール接続を確立するには、V.150 用に SIP で 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。</p> |

SIP トランクセキュリティプロファイルの適用

[Trunk Configuration] ウィンドウでトランクに 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、次の手順を実行します。

- 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、トランクを検索します。
- ステップ 2 [Trunk Configuration] ウィンドウが表示されたら、[SIP trunk Security Profile] の設定を見つけます。

ステップ3 セキュリティプロファイルのドロップダウンリストから、デバイス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、[**Apply Config**] をクリックします。
ダイジェスト認証を有効にしたプロファイルを SIP トランクに適用した場合は、トランクの [SIP レalm (SIP Realm)] ウィンドウでダイジェストログイン情報を設定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は、[**アプリケーションユーザ (Application User)**] ウィンドウでダイジェストクレデンシャルと許可された認可方式を設定する必要があります(まだ実行していない場合)。

Sip トランクセキュリティプロファイルと SIP トランクの同期

SIP トランクを設定変更を行った SIP トランクセキュリティプロファイルと同期するには、次の手順を実行します。これにより、最も影響の少ない方法で未処理の設定が適用されます。(たとえば、影響を受けるデバイスの一部では、リセットまたは再起動が不要な場合があります。)

ステップ1 [System] > [Security Profile] > [SIP Trunk Security Profile] の順に選択します。

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。

ウィンドウに検索条件と一致する 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 該当する SIP トランクを同期する 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 (Apply Configuration Information)] 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。

Cisco Unified Communications Manager Administration を使用した SRTP の許可

[SRTP を許可する (SRTP Allowed)] 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 Trunk (Gatekeeper Controlled) Configuration] ウィンドウ

- [Inter-Cluster Trunk (Gatekeeper Controlled) Configuration] ウィンドウ
- [Inter-Cluster Trunk (Non-Gatekeeper Controlled) Configuration] ウィンドウ
- [SIP トランクの設定 (SIP Trunk Configuration)] ウィンドウ

H.323 ゲートウェイ、ゲートキーパー制御または非ゲートキーパー制御の H.323/H.245/H.225 トランク、SIP トランクの [SRTP Allowed] チェックボックスを設定するには、次の手順を実行します。

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検索します。

ステップ 2 ゲートウェイまたはトランクの設定ウィンドウを開いた後、[SRTP を許可する (SRTP Allowed)] チェックボックスをオンにします。

注意 SIP トランクの [SRTP を許可する (SRTP Allowed)] チェックボックスをオンにする場合は、キーや他のセキュリティ関連の情報がネゴシエーション中に公開されないように TLS 暗号化プロファイルの使用を推奨します。非セキュアプロファイルを使用すると、SRTP は機能しますが、キーはシグナリングおよび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 デバイスをリセットするには、[Reset] をクリックします。

ステップ 5 IPSec が H323 に対して正しく設定されていることを確認します。(SIP の場合は、TLS が正しく設定されていることを確認してください)。



第 16 章

TLS セットアップ

- [TLS の概要 \(233 ページ\)](#)
- [TLS の前提条件 \(233 ページ\)](#)
- [TLS 設定タスク フロー \(234 ページ\)](#)
- [TLS の連携動作と制約事項 \(239 ページ\)](#)

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とデータ転送を実現します。TLS は音声ドメインへのアクセスを防ぐために、ユニファイド コミュニケーション マネージャ 制御システム、デバイス およびプロセス間の接続を保護および制御します。

TLS の前提条件

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、ユニファイド コミュニケーション マネージャ IM およびプレゼンス サービスで設定する 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、メディアターミネーションポイント (MTP)、Xcoder、Prime Collaboration Assurance および Prime Collaboration Provisioning をアップグレードすることはできません。



(注) ユニファイド コミュニケーション マネージャ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。たとえば、ユニファイド コミュニケーション マネージャ IM および プレゼンス サービス 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

TLS 接続の Unified Communications Manager を構成するには、次の作業を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | 最小 TLS バージョンの設定 (235 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。上位のバージョンの TLS がセキュリティ要件で求められる場合は、TLS 1.1 または 1.2 を使用するようにシステムを再設定します。 |
| ステップ 2 | (任意) TLS 暗号化の設定 (235 ページ)。 | Unified Communications Manager でサポートされる TLS 暗号オプションを構成します。 |
| ステップ 3 | SIP トランクのセキュリティ プロファイルでの TLS の設定 (236 ページ)。 | SIP トランクに TLS 接続を割り当てます。このプロファイルを使用するトランクでは、シグナリングのために TLS を使用します。また、セキュア トランクを使用することにより、会議ブリッジなどのデバイスに TLS 接続を追加することができます。 |
| 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 (236 ページ)。 | トランクの TLS サポートを可能にするため、TLS 対応 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ます。また、セキュア トランクを使用することにより、会議ブリッジなどのリソースに接続することができます。 |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| 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 (237 ページ)。 | 電話セキュリティ プロファイルに TLS 接続を割り当てます。このプロファイルを使用する電話では、シグナリングのために TLS を使用します。 |
| ステップ 6 | 電話へのセキュア電話プロファイルの追加 (238 ページ)。 | 作成した TLS 対応プロファイルを電話に割り当てます。 |
| ステップ 7 | ユニバーサル デバイス テンプレートへのセキュア電話プロファイルの追加 (238 ページ)。 | TLS 対応の電話の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。LDAP ディレクトリ同期がこのテンプレートで設定されている場合は、LDAP 同期化を通じて電話の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 の前提条件 \(233 ページ\)](#)」を参照してください。

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。

ステップ 4 すべての Unified Communications Manager と IM and Presence Service クラスタノードで、手順 3 を実行します。

TLS 暗号化の設定

SIP インターフェイスで使用可能な最強の暗号方式を選択することで、弱い暗号を無効にすることができます。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。

-
- ステップ 1** Cisco Unified CM Administration から、[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。
- 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 (Save)] をクリックします。
- (注) すべての TLS 暗号は、クライアントの暗号設定に基づいてネゴシエートされます。
-

SIP トランクのセキュリティ プロファイルでの TLS の設定

SIP トランク セキュリティ プロファイルに TLS 接続を割り当てるには、次の手順を実行します。このプロファイルを使用するトランクでは、シグナリングのために TLS を使用します。

- ステップ 1** Cisco Unified CM の管理から、[システム (System)] > [セキュリティ (Security)] > [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** 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 SIP トランク 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、既存のプロファイルを選択します。
- ステップ 3** [名前 (Name)] 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** [デバイスセキュリティモード (Device Security Mode)] フィールドの値を、[暗号化 (Encrypted)] または [認証 (Authenticated)] に設定します。
- ステップ 5** [受信転送タイプ (Incoming Transport Type)] フィールドと [送信転送タイプ (Outgoing Transport Type)] フィールドの両方の値を、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 (SIP Trunk Security Profile)] ウィンドウの残りのフィールドにデータを入力します。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

TLS 対応の 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るには、次の手順を使用します。このトランクを使用することにより、会議ブリッジなどのリソースとのセキュア接続を作成できます。

-
- ステップ 1 Cisco Unified CM の管理から、[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、既存のトランクを選択します。
- ステップ 3 [デバイス名 (Device Name)] フィールドに、トランクのデバイス名を入力します。
- 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 [SIP プロファイル (SIP Profile)] ドロップダウンリストで、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 (SIP Trunk Security Profile)] ドロップダウンリストボックスから、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 (Destination)] 領域に、宛先 IP アドレスを入力します。最大 16 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 [トランクの設定 (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 9 [保存 (Save)] をクリックします。
- (注) トランクをセキュア デバイスに接続する場合、Unified Communications Manager にセキュア デバイスの証明書を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」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

電話セキュリティ プロファイルに TLS 接続を割り当てるには、次の手順を実行します。このプロファイルを使用する電話では、シグナリングのために TLS を使用します。

-
- 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。
- [新規追加 (Add New)] をクリックして新しい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、既存のプロファイルを選択します。
- ステップ 3 新しいプロファイルを作成する場合は、電話モデルとプロトコルを選択し、[次へ (Next)] をクリックします。
- (注) ユニバーサルデバイス テンプレートと LDAP 同期を使用して LDAP 同期を通じてセキュリティをプロビジョニングする場合は、[電話セキュリティ プロファイル タイプ (Phone Security Profile Type)] に [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 4 プロファイル名を入力します
- ステップ 5 [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 ボックスで、[暗号化 (Encrypted)] または [認証 (Authenticated)] を選択します。
- ステップ 6 (SIP 電話のみ) 転送タイプには、TLS を選択します。

ステップ7 [電話セキュリティプロファイルの設定 (Phone Security Profile Configuration)] ウィンドウ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8 [保存 (Save)] をクリックします。

電話へのセキュア電話プロファイルの追加

TLS 対応の電話セキュリティプロファイルを電話に割り当てるには、次の手順を使用します。



(注) 一度に多数の電話にセキュアプロファイルを割り当てるには、一括管理ツールを使用することにより、それらのセキュリティプロファイルの再割り当てを行います。

ステップ1 Cisco Unified CM の管理から、[デバイス (Device)] > [電話 (Phone)] 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機を作成します。
- [検索 (Find)] をクリックして検索し、既存の電話機を選択します。

ステップ3 電話の種類とプロトコルを選択し、[次 (Next)] をクリックします。

ステップ4 [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から、作成したセキュアプロファイルを電話に割り当てます。

ステップ5 次の必須フィールドに値を割り当てます。

- 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。

ユニバーサル デバイス テンプレートへのセキュア電話プロファイルの追加

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割り当てるには、次の手順を使用します。LDAP ディレクトリ同期が設定されている場合は、機能グループテンプレートとユーザプロファイルにより LDAP 同期にこのユニバーサルデバイス

ンプレートを含めることができます。同期処理が発生すると、電話に対してセキュアプロファイルがプロビジョニングされます。

ステップ 1 [Cisco Unified CM 管理 (Cisco Unified CM Administration)] から、以下を選択します。[**ユーザ管理 (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)**]

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 (Name)] 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 [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から、作成した TLS 対応セキュリティプロファイルを選択します。

(注) [ユニバーサルデバイステンプレート (Universal Device Template)] をデバイスタイプとする電話セキュリティプロファイルが作成されていなければなりません。

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 9 [保存 (Save)] をクリックします。

LDAP ディレクトリ同期処理に、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設定方法の詳細については、『[Cisco Unified Communications Manager システム設定ガイド](#)』の「エンドユーザの設定」部分を参照してください。

TLS の連携動作と制約事項

この章では、TLS のインタラクションと制限事項について説明します。

TLS の相互作用

表 33: TLS の相互作用

| 機能 | 連携動作 |
|--------------|---|
| コモンクライテリアモード | コモンクライテリアモードは、最低限の TLS バージョンの設定と共に有効にすることができます。そのようにする場合、アプリケーションは、引き続きコモンクライテリアの要件に準拠し、アプリケーションレベルで TLS 1.0 セキュア接続を無効にすることになります。コモンクライテリアモードが有効な場合、アプリケーションで最低限の TLS バージョンを 1.1 または 1.2 のいずれかとして設定することができます。コモンクライテリアモードの詳細については、『 <i>Command Line Interface Reference Guide for Cisco Unified Communications Solutions</i> 』の中のコモンクライテリアへの準拠のトピックを参照してください。 |

TLS の制限

79xx、69xx、89xx、99xx、39xx、IP Communicator など、従来型の電話に 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のある問題を、次の表に示します。使用している電話で、このリリースのセキュアモードがサポートされているかどうかを確認するには、Cisco Unified Reporting の Phone Feature List Report を参照してください。従来型の電話の機能制限 および機能を実装するための回避策の一覧を、次の表に示します。



(注) 回避策は、影響を受ける機能が、実際のシステムで動作するように設計されています。しかし、その機能の TLS 1.2 コンプライアンスについては保証できません。

表 34: Transport Layer Security (TLS) バージョン 1.2 の制約事項

| 機能 | 制限事項 |
|---------------|---------------------------------|
| 暗号化モードの従来型の電話 | 暗号化モードの従来型の電話は動作しません。回避策はありません。 |
| 認証モードの従来型の電話 | 認証モードの従来型の電話は動作しません。回避策はありません。 |

| 機能 | 制限事項 |
|---|--|
| <p>HTTPSに基づくセキュア URL を使用する IP 電話サービス。</p> | <p>HTTPS に基づくセキュア URL を使用する IP 電話サービスは動作しません。</p> <p>IP 電話サービスを使用するための回避策：基盤になってい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、社内ディレクトリと個人用ディレクトリ。しかし、エクステンションモビリティなどの機能で、機密データを入力することが必要な場合、HTTP では安全ではないため、HTTP はお勧めしません。HTTP 使用には、次の欠点があります。</p> <ul style="list-style-type: none"> • 従来型の電話に HTTP、サポート対象の電話に HTTPS を設定する場合のプロビジョニングに関する課題。 • IP 電話サービスの復元力の欠如。 • IP 電話サービスを処理するサーバのパフォーマンスが低下する可能性。 |
| <p>従来型の電話でのエクステンション モビリティ クロス クラスタ (EMCC)</p> | <p>EMCC は、従来型の電話の TLS 1.2 でサポートされていません。</p> <p>回避策：EMCC を有効にするため、次の作業を実行します。</p> <ol style="list-style-type: none"> 1. HTTPS ではなく HTTP により 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ます。 3. すべての Unified Communications Manager クラスタに同じ USB eToken を使用します。 |
| <p>従来型の電話でのローカルで有効な証明書 (LSC)</p> | <p>LSC は、従来型の電話の TLS 1.2 で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 認証はご利用いただけません。</p> <p>802.1x のための回避策：古い電話では、MIC または EAP-MD5 によるパスワードに基づく認証。ただし、これらは推奨されません。</p> <p>VPN のための回避策：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。</p> |
| <p>暗号化 Trivial File Transfer Protocol (TFTP) 構成ファイル</p> | <p>暗号化 Trivial File Transfer Protocol (TFTP) 構成ファイルは、メーカーのインストールした証明書 (MIC) がある場合でも、従来型の電話の TLS 1.2 でサポートされません。</p> <p>回避策はありません。</p> |

| 機能 | 制限事項 |
|--|--|
| CallManager 証明書を更新すると、従来型の電話は信頼を失う | <p>従来型の電話は、CallManager 証明書が更新された時点で信頼を失います。たとえば、証明書更新後、電話は新しい構成を取得できなくなります。これは、ユニファイドコミュニケーションマネージャ11.5.1だけで適用されます。</p> <p>回避策：従来型の電話が信頼を失わないようにするため、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. CallManager 証明書を有効にする前に、[8.0 より前のリリースヘルロールバックするクラスター (Cluster For Roll Back to Pre 8.0)] エンタープライズパラメータを True に設定します。デフォルトでは、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 (ユニファイドコミュニケーションマネージャを複数回リブート)。 |
| サポートされていないバージョンの Cisco Unified Communications Manager への接続 | <p>より高い TLS バージョンをサポートしていない Unified Communications Manager の古いバージョンへの TLS 1.2 接続は動作しません。たとえば、Unified Communications Manager リリース 9.x への TLS 1.2 SIP トランク接続は動作しません。このリリースでは TLS 1.2 がサポートされていないためです。</p> <p>次の回避策のいずれかを使用できます。</p> <ul style="list-style-type: none"> • 接続を有効にするための回避策：非セキュア トランクを使用。ただし、推奨されるオプションではありません。 • TLS 1.2 を使用しつつ接続を有効にするための回避策：TLS 1.2 をサポートしていないバージョンから、サポートするリリースにアップグレードします。 |
| Certificate Trust List (CTL) クライアント | <p>CTL クライアントでは、TLS 1.2 がサポートされません。</p> <p>次の回避策のいずれかを使用できます。</p> <ul style="list-style-type: none"> • CTL クライアントを使用する際に一時的に TLS 1.0 を許可し、クラスターをコモンクライテリアモードに移します。最小 TLS を 1.1 または 1.2 に設定します • コモンクライテリアモードで CLI コマンド utils ctl set-cluster mixed-mode を使用することにより、Tokenless CTL に移行します。最小 TLS を 1.1 または 1.2 に設定します |
| アドレス帳同期 | 回避策はありません。 |

Cisco Unified Communications ManagerIM およびプレゼンスサービスのポートのうち Transport Layer Security Version 1.2 によって影響を受けるもの

次の表に、TLS バージョン 1.2 の影響を受ける Unified Communications Manager ポートを示します。

表 35: Cisco Unified Communications Manager のポートのうち Transport Layer Security Version 1.2 によって影響を受けるもの

| アプリケーション | プロトコル | 宛先/リスナー | 通常モードで動作する Cisco Unified Communications Manager | | | コモンクライトリアモードで動作する Cisco Unified Communications Manager | | |
|---|---|---------|---|------------------|------------------|--|------------------|------------------|
| | | | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 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-秒-SIG | Signalling Connection Control Part (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 |
| コンピュータテレフォニー インテグレーション (CTI) [コンピュータテレフォニー インテグレーション CTI] | Quick Buffer Encoding (QBE) [Quick Buffer Encoding] | 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 |

| アプリケーション | プロトコル | 宛先/リスナー | 通常モードで動作する Cisco Unified Communications Manager | | | コモンクライトリアモードで動作する Cisco Unified Communications Manager | | |
|--------------------------|--------------------------------------|------------------|---|------------------------|------------------|--|------------------------|------------------|
| | | | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 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 |
| クラスタ間検索サービス (ILS) | N/A | 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 |
| Administrative XML (AXL) | Simple Object Access Protocol (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 (HAProxy) | 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 (トランクで設定可能) | 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 Proxy | TCP | 6971、6972 | TLS 1.2 | TLS 1.2 | TLS 1.2 | TLS 1.1 | TLS 1.1、TLS 1.2 | TLS 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 |
| 信頼検証サービス (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 Presence のポートのうち Transport Layer Security バージョン 1.2 による影響を受けるもの

次の表は、Transport Layer Security バージョン 1.2 の影響を受ける IM and Presence Service ポートを示します。

表 36: インスタントメッセージングと Presence のポートのうち Transport Layer Security バージョン 1.2 による影響を受けるもの

| 宛先/リスナー | 通常モードで動作するインスタントメッセージングと Presence | | | コモンクライテリアモードで動作するインスタントメッセージングと Presence | | |
|---------|-----------------------------------|---------------------|------------------|--|---------------------|------------------|
| | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 TLS バージョン 1.2 | 最低 TLS バージョン 1.0 | 最低 TLS バージョン 1.1 | 最低 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 |
| 7335 | 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

- [ID の管理 \(249 ページ\)](#)
- [クレデンシャル ポリシー \(257 ページ\)](#)
- [連絡先検索認証 \(267 ページ\)](#)



第 17 章

ID の管理

- ユーザセキュリティの概要 (249 ページ)
- アイデンティティ管理の概要 (250 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、ユーザ、エンドポイント、およびオンラインアクティビティを保護して、より効率的にリスクを関連付けるプラットフォームで構成されています。ユーザがパーソナルデバイスを介してネットワークにログインする傾向がある中で、パーソナルデバイスのセキュリティ保護は、会社が所有するデバイスのセキュリティ保護と同様に重要です。

ユーザ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。

Unified Communications Manager でユーザアクセスを管理するロールに関連付けられているアクセス制御グループにエンドユーザを割り当てます。

アクセス制御は、基本的に、適切なユーザがネットワークにアクセスできるようにすると同時に不適切なユーザをブロックすることができます。アクセス制御は、ネットワークにアクセスしているユーザとデバイスを把握する機能です。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ます。アクセス制御は情報の拡散を制限し、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。

ロールとアクセス制御グループは、Unified Communications Manager に対して複数のレベルのセキュリティを提供します。各ロールは、Unified Communications Manager 内の特定のリソースに対する一連の権限を定義します。ロールをエンドユーザに割り当てて、エンドユーザをアクセス制御グループに割り当てると、エンドユーザーはそのロールによって定義されたアクセス許可を取得します。

インストールの際、Unified Communications Manager は定義済みのデフォルトアクセス制御グループに割り当てられた定義済みのデフォルトロールを備えています。エンドユーザをデフォ

ルトのアクセス制御グループに割り当てることも、新しいアクセス制御グループとロールを設定してアクセス設定をカスタマイズすることもできます。

ユーザとアクセス制御の詳細については、『[Cisco Unified Communications Manager システム設定ガイド](#)』の「[エンドユーザの設定](#)」と『[Cisco Unified Communications Manager アドミニストレーションガイド](#)』の「[ユーザの管理](#)」を参照してください。

ID の管理

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 では、信頼できるビジネスパートナー間で、セキュリティに関連した情報交換を記述します。これは、ユーザを認証するために、サービスプロバイダー (Cisco Unified Communications Manager など) が使用する認証プロトコルです。SAML を使用して、アイデンティティプロバイダーとサービスプロバイダーがセキュリティ認証情報を交換します。この機能が安全なメカニズムを提供していることで、さまざまなアプリケーションにわたり、共通のログイン情報や関連情報を使用します。アイデンティティ管理の詳細については、[Cisco Unified Communications Manager アドミニストレーションガイド](#)の「[SAML シングルサインオンの管理](#)」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、他のユーザをディレクトリで検索する前に、ユーザ自身を認証する必要があります。連絡先検索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. [連絡先検索の認証の電話サポートの確認 \(268 ページ\)](#)
2. [連絡先検索の認証の有効化 \(268 ページ\)](#)
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 \(268 ページ\)](#)

アイデンティティ管理の概要

アイデンティティ管理は、シスココラボレーション導入に必須のコンポーネントです。アイデンティティは多くの場合、ハッカーの主なターゲットとなるため、システムを保護するには、セキュア認証および許可サービスを設定する必要があります。Cisco Unified Communications Manager には、サービスのアイデンティティ、認証、および許可を管理するための複数のオプションがあります。

- サードパーティ アイデンティティ プロバイダーによる SAML SSO の導入
- LDAP 認証
- ローカル DB 認証

SAML SSO の展開

SAML SSO により、企業のセキュリティが向上すると同時に、生産性が向上します。SAML 2.0 プロトコルを使用して、SAML SSO はシスコ コラボレーション インフラストラクチャをサードパーティ アイデンティティ プロバイダーに接続し、ドメイン全体や製品全体にわたって管理者およびクライアントのログイン用のセキュアなログインおよび認証サービスを提供します。アイデンティティ プロバイダーが単一のログインを保存しているため、ワーカーの生産性が向上します。Collaboration 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しにこれらのアプリケーションにアクセスできます。

SAML SSO は、アイデンティティ フレームワークに次の利点があります。

- 異なるユーザ名およびパスワードの組み合わせを入力する必要がなくなり、パスワードによる疲労が軽減されます。
- アプリケーションをホストしている自社システムからサードパーティのシステムに、認証を転送できます。
- 認証情報を保護して、安全性が向上します。SAML SSO は、暗号化機能により、IdP、サービスプロバイダー、およびユーザ間で転送される認証情報を保護します。SAML SSO では、IdP とサービス プロバイダー間で転送される認証メッセージを外部ユーザから保護することもできます。
- 同じアイデンティティのログイン情報を再入力する時間が省けるため、生産性が向上します。
- パスワードをリセットするためのヘルプデスクへの問い合わせが減るため、コスト削減につながります。

IdP との信頼関係

SAML SSO の導入は、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 の関係を設定できます。

- ノード単位の契約 : UC メタデータ zip ファイルには、ノードごとに別々の XML ファイルが含まれています。
- クラスタごとの契約 : クラスタ用の単一のメタデータファイル

この信頼関係は、最初のメタデータファイルの交換によって作成されます。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
- Organization
- この情報の有効期限
- キャッシング期間
- この情報の XML 署名

- 担当者
- エンティティの一意的識別子（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 プロバイダー、サービス プロバイダーなど）

許可

IdP によって認証されると、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ているアクセス制御グループと、それらのグループが提供するロールの権限によって決定されます。

SAML SSO の設定とアイデンティティ プロバイダーの要件

アイデンティティプロバイダーの設定情報や要件など、SAML SSOの詳細については、『*SAML SSO Deployment Guide for Cisco Unified Communications Applications*』を参照してください。

LDAP 認証

SAML SSO を導入しなかった場合に、ユーザを会社の LDAP ディレクトリと同期している場合、LDAP 認証により、会社の LDAP ディレクトリに保存されているログイン情報に対してユーザ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 のアイデンティティ管理システム（IMS）ライブラリは、LDAP が同期されたユーザのユーザパスワードを認証するために、会社の LDAP ディレクトリを使用できます。

エンドユーザは、セルフケアポータルにログインするときに、会社の LDAP ディレクトリで設定されている会社パスワード（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、シンプルバインド操作によって社内ディレクトリに対して認証される。
- 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る。
- アプリケーション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る。
- エンドユーザ PIN は、Unified CM データベースに対して認証される。

LDAP 認証の設定

エンドユーザパスワードの LDAP 認証を有効にするには、次の手順を使用します。既存の LDAP ディレクトリ同期に LDAP 認証を追加できます。

始める前に

この手順では、LDAP ディレクトリ同期がすでに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まだ設定していない場合は、『System Configuration Guide for Cisco Unified Communications Manager』を参照して同期を設定してください。

- ステップ 1 Cisco Unified CMの管理で、システム > LDAP > LDAP検索 を選択します。
- ステップ 2 [エンドユーザに LDAP 認証を使用する (Use LDAP Authentication for End Users)] チェックボックスをオンにします。
- ステップ 3 [LDAP マネージャの識別名 (LDAP Manager Distinguished Name)] として、該当する LDAP ディレクトリへのアクセス権を持つ管理ユーザである LDAP Manager の ユーザ ID を入力します。
- ステップ 4 [パスワード (Password)] と [パスワードの確認 (Confirm the Password)] にパスワードを入力します。
- 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、残りのフィールドに入力します。
- 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

サードパーティアイデンティティプロバイダーを使用して SAML SSO を導入しない場合、または LDAP 認証が設定されていない場合は、エンドユーザに対して Cisco Unified Communications Manager データベースに対するローカル認証が必要です。このオプションでは、ユーザパスワードがローカルデータベースに保存され、エンドユーザ設定によって管理されます。

アプリケーションユーザとエンドユーザの PIN の両方について、ローカルデータベース認証は常に認証の管理に使用されます。次の表に、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:

| パスワードタイプ | クレデンシャル管理 |
|-------------|---|
| エンドユーザパスワード | SAML SSO または LDAP 認証を使用しない場合は、エンドユーザパスワードは個々のエンドユーザの [エンドユーザ設定 (End User Configuration)] 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で自分のパスワードを編集できます。 |
| エンドユーザ PIN | SAML SSO や LDAP 認証の導入にかかわらず、エンドユーザの PIN は、Cisco Unified CM Administration の [エンドユーザ設定 (End User Configuration)] ウィンドウで常に管理されます。 管理者は、[エンドユーザ設定 (End User Configuration)] ウィンドウで既存のエンドユーザの PIN を編集できます。 |

| パスワードタイプ | クレデンシャル管理 |
|------------------|--|
| アプリケーションユーザパスワード | SAML SSO や LDAP 認証の導入に関係なく、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設定 (Application User Configuration)] 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、IETF の RFC 6749 で定義されています。OAuth 2.0 認証プロトコルでは、リソース所有者 (Cisco Unified Communications Manager など) は、サードパーティ製アプリケーションが HTTP サービスへの制限されたアクセスを取得するのを許可することができます。Cisco Unified Communications Manager を使用すると、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許可し、トークンを更新してトークンの有効期限を越えてリソースにアクセスできるようにすることができます。OAuth を使用すると、ユーザが情報にアクセスしようとするときに Web サイトでパスワードの入力を求める必要がなくなります。OAuth を使用すると、クライアントがサーバー上のリソースにアクセスするのをユーザー自身が許可します。

Cisco Jabber クライアントは、OAuth 更新ログインを使用して Cisco Unified Communications Manager からリソースにアクセスします。最初のログイン後に、OAuth アクセストークンと更新トークンは、トークンの有効期限を越えて、リソースへのシームレスなアクセスを提供します。

OAuth 更新ログイン

OAuth 更新ログインを使用すると、短い有効期限のアクセストークンによって Jabber を認証し、トークンの有効期限が有効である間、アクセスを許可します (アクセストークンのデフォルトの有効期限は 60 分です)。期間の長い更新トークンは、古いアクセストークンが期限切れになったときに、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ます。これにより、ユーザは再認証する必要なしにシームレスにアクセスできます。

OAuth トークンが有効期間の 75% に達するたびに、エンドユーザー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 はエンドユーザーを承認する新しいアクセストークンを提供します。更新トークンが存続期間の 100% に達した場合は、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。



重要 この機能は、リリース 15 以降の Webex クライアントにのみ適用されます。

Webex クライアントがアクセストークンの更新を要求するたびに、Cisco Unified Communications Manager は、更新トークンの更新機能が Cisco Unified CM および Webex クライアントで有効になっているかどうか、および更新トークンの有効期間が有効期限の 50% に達しているかどうかを確認します。両方の条件が満たされると、アクセストークンの更新プロセス中に更新トークンが自動的に更新され、再認証を必要としないシームレスなアクセスが保証されます。

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することで、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 モードにより、CAPF なしで Jabber のセキュアな署名とメディアが可能になります。SIP 登録中にトークンの検証が完了します。このモードでは、Jabber は LSC なしで、また、統一された CM で混合モードを有効にする必要なしに、メディアおよびシグナリングの暗号化を実行できます。

OAuth のキーの再生成

署名と OAuth トークンの暗号化に使用されるキーが侵害されたと思われる場合は、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。

- `set key regen authz encryption`
- `set key regen authz 署名`



(注) OAuth キーが再生成されたら、Jabber OAuth ログインを機能させるために、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 回線の OAuth 更新ログインを使用できるよう SIP OAuth モードを設定する方法の詳細については、『*Feature Configuration Guide for Cisco Unified Communications Manager*』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>
```

引数の説明

- `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 Manager 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 18 章

クレデンシャル ポリシー

- [クレデンシャル ポリシーの概要 \(257 ページ\)](#)
- [デフォルトのクレデンシャル ポリシーの設定 \(259 ページ\)](#)
- [エンドユーザログイン情報またはログイン情報ポリシーの編集 \(260 ページ\)](#)
- [PIN同期の有効化 \(261 ページ\)](#)
- [認証アクティビティのモニタ \(262 ページ\)](#)
- [クレデンシャル キャッシングの設定 \(263 ページ\)](#)
- [セッションの終了の管理 \(264 ページ\)](#)

クレデンシャル ポリシーの概要

クレデンシャル ポリシーは、Cisco Unified Communications Manager 内のリソースの認証プロセスを制御します。クレデンシャルポリシーは、失敗したログイン試行、エンドユーザパスワードの有効期限とロックアウト期間、エンドユーザ PIN、アプリケーションユーザパスワードなどのパスワード要件とアカウントロックアウトの詳細を定義します。クレデンシャルポリシーは、すべてのエンドユーザ PIN などの特定のクレデンシャルタイプのすべてのアカウントに広く割り当てることも、特定のアプリケーションユーザやエンドユーザ用にカスタマイズすることもできます。

クレデンシャルタイプ

[クレデンシャルポリシー設定 (Credential Policy Configuration)] で、新しいクレデンシャルポリシーを設定し、次の 3 つのクレデンシャルタイプのそれぞれのデフォルト クレデンシャルポリシーとして新しいポリシーを適用できます。

- エンドユーザ PIN
- エンドユーザパスワード
- アプリケーションユーザパスワード

また、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クレデンシャルポリシーを適用することもできます。

LDAP 認証が有効になっている場合のログイン情報ポリシー

社内ディレクトリで LDAP 認証用にシステムが設定されている場合は、次の条件を実行します。

- LDAP 認証が有効になっている場合、ログイン情報ポリシーはエンドユーザパスワードに適用されません。
- ログイン情報ポリシーは、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パスワードに適用されます。これらのパスワードタイプは、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

単純なパスワードと PIN を確認するようにシステムを設定できます。単純なパスワードとは、ABCD や 123456 といった容易に推測できるパスワードなどで、これらは簡単にハッキングできるクレデンシャルです。

単純でないパスワードは、次の要件を満たしています。

- 大文字、小文字、数字、記号の 4 種類の文字のうち 3 種類を含んでいる。
- 3 回以上連続して同じ文字や数字を使用していない。
- 繰り返しや、エイリアス、ユーザ名、内線番号を含んでいない。
- 連続する文字または数字で構成されていない。たとえば、654321 または ABCDEFG などのパスワードは許容されません。

PIN には、数字 (0 ~ 9) のみを使用できます。単純でない PIN は、次の条件を満たすものとします。

- 3 回以上連続して同じ数字を使用していない。
- 繰り返しや、ユーザの内線番号、メールボックス、またはユーザの反転させた内線番号やメールボックスを含んでいない。
- 3 つの異なる数字を含んでいる。たとえば、121212 などの PIN は単純です。
- ユーザの姓または名の数字表現 (たとえば、名前によるダイヤル) が使用されていない。
- たとえば、408408 などの複数の数字の繰り返しや、2580、159、753 などのキーパッド上で直線上にあるダイヤルのパターンを含んでいない。

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のためのロックアウト戻りコードにตอบสนอง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、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-programming-reference-guides-list.html> にある開発者ガイド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クレデンシャルポリシーを設定するには、次の手順を使用します。次の各ログイン情報タイプに対して、個別のログイン情報ポリシーを適用できます。

- アプリケーション ユーザ パスワード
- エンドユーザのパスワード
- エンドユーザ PIN

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 から、**[ユーザ管理 (User Management)]** > **[ユーザ設定 (User Settings)]** > **[クレデンシャルポリシー (Credential Policy)]** 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 (Save)]** をクリックします。
- f) 他のクレデンシャルタイプのいずれかに対して異なるクレデンシャルポリシーを作成する場合は、これらの手順を繰り返します。

ステップ 2 クレデンシャルポリシーをクレデンシャルタイプのいずれかに適用します。

- a) Cisco Unified CM Administration から、[ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [クレデンシャルポリシーのデフォルト (Credential Policy Default)] 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することもできます。
- 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。ユーザは次のログイン時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 (Save)] をクリックします。
- g) 他のクレデンシャルタイプのいずれかにクレデンシャルポリシーを割り当てる場合は、これらの手順を繰り返します。



- (注) 個人ユーザに対して、[エンドユーザの設定 (End User Configuration)] 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の設定 (Application User Configuration)] ウィンドウから、特定のユーザログイン情報にポリシーを割り当てることもできます。ログイン情報タイプ (パスワードまたは PIN) の隣にある [ログイン情報の編集 (Edit Credential)] ボタンをクリックして、そのユーザログイン情報に関する [ログイン情報の設定 (Credential Configuration)] を開きます。

エンドユーザログイン情報またはログイン情報ポリシーの編集

既存のユーザログイン情報を編集する場合、またはユーザログイン情報に割り当てられたポリシーを編集する場合は、次の手順を実行します。ログイン情報をリセットした後は、次のログイン時にユーザがログイン情報を更新する必要があるなどのルールを適用できます。次の場合にこれを行います。

- ローカル DB 認証が設定されている場合にエンドユーザパスワードをリセットする
- 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する
- 特定のユーザログイン情報に割り当てられたログイン情報ポリシーを変更する

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、[ユーザ管理 (User Management)] > [エンドユーザ (End Users)] を選択します。
- アプリケーションのユーザパスワードの場合は、[ユーザの管理 (User Management)] > [アプリケーション ユーザ (Application User)] を選択します。

ステップ 2 [検索 (Find)] をクリックして、該当する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、[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)] フィールドに新しいログイン情報を入力し、[保存 (Save)] をクリックします。

ステップ 4 ユーザのログインに割り当てられたログイン情報ポリシーを変更する場合、または次のログイン時にユーザ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は、次の手順を実行します。

- a) [パスワード (Password)] または [PIN] の隣にある [ログイン情報の編集 (Edit Credential)] ボタンをクリックします。そのユーザログイン情報の [ログイン情報の設定 (Credential Configuration)] ウィンドウが開きます。
- b) オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。新しいログイン情報ポリシーを割り当てるには、[認証ルール (Authentication Rule)] ドロップダウンリストからポリシーを選択します。
- c) オンプレミスの場合、HTTPのデフォルトは8090、HTTPSのデフォルトは8181です。次のログイン時にパスワードまたは PIN を更新するようにユーザに求める場合は、[ユーザは次のログイン時に変更する必要があります (User Must Change at Next Login)] チェックボックスをオンにします。
- 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 の管理 (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 ID と一致する必要があります。

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 [エンドユーザーの 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タ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。

ステップ 1 [Cisco Unified CM の管理 (Cisco Unified CM Administration)]>[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。また、キャプチャしたイベントをレポートに収集できます。Unified RTMT の詳細な使用手順については、<http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html> にある『Cisco Unified Real-Time Monitoring Tool アドミニストレーション ガイド』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、ストアー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ア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。

ステップ 1 Cisco Unified CM の管理から、[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。

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アルを使用します。
- システムがキャッシュされたクレデンシア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。クレデンシア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。

セッションの終了の管理

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 Reporting
- Cisco Unified Communications セルフ ケア ポータル
- Cisco Unified CM IM and Presence の管理
- Cisco Unified IM and Presence サービスアビリティ
- Cisco Unified IM and Presence のレポート

-
- 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 19 章

連絡先検索認証

- [連絡先検索認証の概要 \(267 ページ\)](#)
- [連絡先検索認証タスクフロー \(267 ページ\)](#)

連絡先検索認証の概要

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分で認証することで、システムのセキュリティを強化します。この機能により、ディレクトリが外部関係者によってアクセスされるのを保護します。

連絡先検索認証タスクフロー

Unified Communications Manager で連絡先検索の認証をセットアップするには、次のタスクを実行します。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ユーザ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 | 連絡先検索の認証の電話サポートの確認 (268 ページ) | 電話でこの機能がサポートされていることを確認します。Cisco Unified Reporting で [Unified CM Phone FeatureList] レポートを実行し、この機能をサポートしている電話モデルのリストを確認します。 |
| ステップ 2 | 連絡先検索の認証の有効化 (268 ページ) | Unified Communications Manager で連絡先検索の認証を設定します。 |
| 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 (268 ページ) | 電話のユーザがディレクトリで他のユーザを検索したときに示される URL を Unified Communications Manager で設定するには、次の手順を実行します。 |

連絡先検索の認証の電話サポートの確認

導入環境内の電話が連絡先検索の認証をサポートしていることを確認します。[Phone Feature List] レポートを実行して、この機能をサポートしているすべての電話モデルのリストを取得します。

- 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 [ユニファイド CM 電話機能 (Unified CM Phone Feature)] を選択します。
- ステップ 3 [ユニファイド 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ます。
- ステップ 5 [機能 (Feature)] ドロップダウンから [Authenticated Contact Search] を選択します。
- ステップ 6 [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認証を設定するには、Unified Communications Manager で次の手順を使用します。

- 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 の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 がユーザ検索リクエストを送信するディレクトリサーバ URL を Unified Communications Manager に設定するには、次の手順を使用します。デフォルトの値は `https://<cucm-fqdn-or-ip>:port/cucm-uds/users` です。



(注) デフォルトの UDS ポートは 8443 です。連絡先検索の認証が有効になると、デフォルトの UDS ポートは 9443 に切り替わります。その後、連絡先検索の認証を無効にした場合は、UDS ポートを手動で 8443 に戻す必要があります。

ステップ 1 Cisco Unified Communications Manager Administration から、[システム (System)] > [エンタープライズパラメータ (Enterprise Parameter)] 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 モードの設定 (273 ページ)
- V.150 の最小必須要件 (289 ページ)
- IPSec の設定 (301 ページ)
- CTI、JTAPI、および TAPI の認証および暗号化の設定 (303 ページ)
- セキュアな録音とモニタリング (319 ページ)
- VPN クライアント (321 ページ)
- オペレーティングシステムとセキュリティの強化 (335 ページ)



第 20 章

FIPS モードの設定

- FIPS 140-2 の設定 (273 ページ)
- 強化されたセキュリティ モード (281 ページ)
- コモンクライテリア モード (284 ページ)

FIPS 140-2 の設定



注意 FIPS モードは、FIPS 準拠のリリースだけでサポートされます。Unified Communications Manager の FIPS 非準拠のバージョンにアップグレードする前に、必ず FIPS モードを無効にしてください。

FIPS 準拠のリリースと、そのリリースの証明書を確認するには、<https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html> の FIPS 140 のドキュメントを参照してください。

連邦情報処理標準 (FIPS) は、米国およびカナダ政府の認証規格です。暗号化モジュールで順守する必要がある要件が規定されています。

Unified Communications Manager の特定のバージョンは、米国の National Institute of Standards (NIST) に従って FIPS 140-2 に準拠しています。これらは FIPS モード、レベル 1 に準拠して動作できます。

Unified Communications Manager

- 再起動
- スタートアップ時に認定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する
- キー情報を再生成する

FIPS 140-2 モードを有効にすると、この時点で、Unified Communications Manager は FIPS 140-2 モードで動作しています。

FIPS の要件には、次のものが含まれます。

- スタートアップ時のセルフテストの実行
- 一連の承認済み暗号機能に対する制限

FIPS モードでは、次の FIPS 140-2 レベル 1 検証済み暗号化モジュールが使用されます。

- CiscoSSL - 1.1.1t.7.2.500 with FIPS Module CiscoSSL FOM 7.2a
- CiscoSSH - 1.10.32
- BC FIPS -1.0.2.3.jar
- BCTLS FIPS - 1.0.12.3.jar
- BCPKIX FIPS -1.0.5.jar
- Strongswan - 5.9.8
- KFOM : linux_kfom_1_0_0



- (注) Unified Communications Manager アップグレードの詳細については、『[Cisco Unified Communications Manager および IM and Presence Service インストール ガイド](#)』の「COP ファイルインストールガイド」セクションを参照してください。

次の FIPS 関連作業を実行できます。

- FIPS 140-2 モードの有効化
- FIPS 140-2 モードの無効化
- FIPS 140-2 モードのステータスの確認



- (注)
- デフォルトでは、システムは非 FIPS モードになっているため、有効にする必要があります。
 - クラスタ上で FIPS、コモンクライテリア、または強化されたセキュリティ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最小 14 文字である必要があります。旧バージョンが FIPS を有効にしていた場合でもパスワードを更新します。

FIPS モードで自己署名証明書または証明書署名要求 (CSR) を生成する場合は、SHA256 ハッシュアルゴリズムを使用して証明書を暗号化する必要があり、SHA1 を選択できません。

FIPS 140-2 モードの有効化

Unified Communications Manager で FIPS 140-2 モードを有効にする前に、次の点を検討してください。

- 非 FIPS モードから FIPS モードに切り替えた場合は、MD5 および DES プロトコルは機能しません。
- 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、または [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は、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。
- クラスタでは、すべてのノードが FIPS モードまたは非 FIPS モードである必要があります。異なるモードの各ノードは許可されません。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。
- FIPS モードをサーバで有効にした後は、サーバがリブートし、電話が正常に再登録されるまで待機してから、次のサーバで FIPS を有効にしてください。
- Unified Communications Manager リリース 15 で FIPS モードを有効にすると、3DES アルゴリズムは IPsec 通信でサポートされません。
- ESP および 3DES として暗号化アルゴリズムを使用して IPsec ポリシーをすでに設定しており、FIPS モードを有効にしている場合は、Unified Communications Manager リリース 15 へのアップグレードがブロックされます。
- リリース 15 へのアップグレードまたは移行を計画している場合は、3DES アルゴリズムを使用した IPsec ポリシーが FIPS モードでサポートされていないことに注意してください。IPsec トンネルが確立される両方のノードで、3DES 以外の暗号化および ESP アルゴリズムを使用して IPsec ポリシーを削除して再作成し、アップグレードまたは移行を計画する必要があります。

**注意**

FIPS モードを有効にする前に、システムバックアップを実行することを強く推奨します。FIPS のチェックが起動時に失敗した場合は、システムが停止し、復元するにはリカバリ CD が必要になります。

展開時に、すべてのクラスタノードが 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ます。クラスタ内に混合ノードをデプロイすることはできません。クラスタは、FIP ノードまたは非 FIPS ノードのいずれかである必要があります。

ステップ 1 CLI セッションを開始します。

詳細については、『[Command Line Interface Reference Guide for Cisco Unified Communications Solutions](#)』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 enable` を入力します。

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、コモンライテリア、強化されたセキュリティモードなどのセキュリティモードを有効にするには、クラスタセキュリティパスワードは 14 文字以上使用する必要があります。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 セキュリティ パスワードを更新し、このコマンドを再実行します。
*****
***** コマンドの実行に失敗しました (Executed command unsuccessfully)
```

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：この操作により、1)CallManager 2)Tomcat 3)IPsec 4)TVS 5)CAPF 6)SSH 7)ITLRecovery
の証明書が再生成されます。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の CA 署名付き証明書
を再アップロードする必要があります。(The operation will regenerate certificates for 1)CallManager
2)Tomcat 3)IPsec 4)TVS 5)CAPF 6)SSH 7)ITLRecovery Any third party CA signed certificates
that have been uploaded for the above components will need to be re-uploaded.) システムが
混合モードで動作している場合は、ctl ファイルを更新するために CTL クライアントを再実行する必要があります。
クラスタ内に他のサーバがある場合は、このノードの FIPS 操作が完了してシステムがバックアップおよび実行
されるまで待機して、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の [TFTP
ファイル署名アルゴリズム (TFTP File Signature Algorithm) ] に Unified Communications Manager
の現行バージョンの FIPS 準拠ではない値 [SHA-1] が設定されている場合は、完全に FIPS にするために、パ
ラメータ値を SHA-512 に変更することを推奨します。SHA-512 を署名アルゴリズムとして設定するには、クラス
タにプロビジョニングされているすべての電話機が SHA-512 署名付き設定ファイルを検証できる必要がある場合が
あります。そうでない場合、電話機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、再起動します。
```

```
***** 警告：続行
したら、Ctrl+C キーを押さないでください。開始後にこの操作をキャンセルすると、システムは一貫性のない状態
になります。リカバリするには、システムをリブートし、「utils fips status」を実行する必要があります。
(Once you continue do not press Ctrl+C. Canceling this operation after it starts will
leave the system in an inconsistent state; rebooting the system and running "utils fips
status" will be required to recover.)
***** Do you
want to continue (yes/no)?
```

ステップ 3 Yes と入力します。

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 mode enabled
successfully. システムのバックアップが実行されると、システムを再起動した後に、これを強くお勧めします。
システムは数分で再起動します。
```

Unified Communications Manager が自動的にリブートされます。

- (注)
- 証明書および SSH キーは、FIPS 要件に応じて、自動的に再生成されます。
 - 単一のサーバクラスタを使用しており、[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てから FIPS 140-2 モードを有効にした場合は、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。
 - クラスタで FIPS を有効にするには、最初にパブリッシャを有効にし、設定されたすべてのサービスが適切に初期化されていることを確認します。次に、クラスタ内の他のすべてのノードで fips を順番に有効にします。

CiscoSSH サポート

Unified Communications Manager は CiscoSSH をサポートします。システムで FIPS モードを有効にすると、CiscoSSH は自動的に有効になります。追加設定は不要です。

CiscoSSH サポート

CiscoSSH は、次のキー交換アルゴリズムをサポートします。

- **Diffie-Hellman-Group14-SHA1**
- **Diffie-Hellman-Group-Exchange-SHA256**
- **Diffie-Hellman-Group-Exchange-SHA1**

CiscoSSH は、Unified Communications Manager サーバで次の暗号をサポートしています。

- **AES-128-CTR**
- **AES-192-CTR**
- **AES-256-CTR**
- **AES-128-GCM@openssh.com**
- **AES-256-GCM@openssh.com**
- **AES-128-CBC** (リリース 12.0(1) 以降をサポート)
- **AES-192-CBC** (リリース 12.0(1) 以降をサポート)
- **AES-256-CBC** (リリース 12.0(1) 以降をサポート)

CiscoSSH は、クライアントの次の暗号方式をサポートします。

- **AES-128-CTR**
- **AES-192-CTR**
- **AES-256-CTR**
- **AES-128-GCM@openssh.com**

- **AES-256-GCM@openssh.com**
- **AES-128-CBC**
- **AES-192-CBC**
- **AES-256-CBC**

FIPS 140-2 モードの無効化

FIPS 140-2 モードを Unified Communications Manager で無効にする前に、次の点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のサーバクラスタで実行されていない場合は、FIPS モードを無効にした後で、手動で ITL ファイルを削除する必要があります。
- 複数サーバのクラスタでは、各サーバを個別に無効にする必要があります。これは、FIPS モードはクラスタ全体ではなくサーバごとに無効になるためです。

FIPS 140-2 モードを無効にするには、次の手順を実行します。

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 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 セッションを開始する」の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 がリブートされ、非 FIPS モードに戻ります。

(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、次の手順を実行します。

ステップ 1 CLI セッションを開始します。

詳細については、『[Command Line Interface Reference Guide for Cisco Unified Communications Solutions](#)』の「Starting a CLI Session」の項を参照してください。

ステップ 2 CLI に **utils fips status** と入力します。

FIPS 140-2 モードが有効になっていることを確認するために、次のメッセージが表示されます。

```
admin:utils fips status The system is operating in FIPS mode. Self test status: - S T A
R T ----- Executing FIPS selftests runlevel is graphical.target Start
time: Wed Aug 2 18:28:56 IST 2023 NSS self tests passed. Kernel Crypto tests passed.
Operating System OpenSSL self tests passed. Strongswan self tests passed. OpenSSL self
tests passed. CryptoJ self tests passed. BCFIPS self tests passed. KFOM self tests passed.
```

FIPS 140-2 モードサーバのリポート

FIPS 140-2 モードで Unified Communications Manager サーバがリポートすると、リポート後に各 FIPS 140-2 モジュールで FIPS のスタートアップ時のセルフテストがトリガーされます。



注意 これらのセルフテストのいずれかが失敗すると、Unified Communications Managerサーバが停止します。



(注) 対応する CLI コマンドを使用して FIPS を有効または無効にすると、Unified Communications Managerサーバが自動的に再起動されます。リポートを開始することもできます。



注意 一時的なエラーによってスタートアップセルフテストに失敗した場合は、Unified Communications Managerサーバの再起動によって問題が修正されます。ただし、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ため、リカバリ CD の使用が唯一の選択肢となります。

FIPS モードの制約事項

| 特長 | 機能制限 |
|------------|--|
| SNMP v3 | FIPS モードでは、MD5 または DES を使用した SNMP v3 はサポートされていません。FIPS モードが有効になっているときに SNMP v3 が設定されている場合は、認証プロトコルとして SHA を設定し、プライバシープロトコルとして AES128 を設定する必要があります。 |
| 証明書のリモート登録 | FIPS モードでは、証明書のリモート登録はサポートされていません。 |

| 特長 | 機能制限 |
|-----------------|---|
| SFTP サーバ | <p>デフォルトでは、JSCH ライブラリは SFIPS 接続に ssh-rsa を使用していましたが、FIPS モードは ssh-rsa をサポートしません。CentOS の最近の更新により、JSCH ライブラリは、変更後の FIPS 値に応じて、ssh-rsa (SHA1withRSA) または rsa-sha2-256 (SHA256withRSA) の両方をサポートします。具体的には、次の選択を行います。</p> <p>(注)</p> <ul style="list-style-type: none"> • 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 と rsa-sha2-256 の両方をサポートします。 <p>rsa-sha2-256 (SHA256WithRSA) のサポートは OpenSSH 6.8 バージョン以降でのみ利用可能です。FIPS モードでは、OpenSSH 6.8 バージョン以降で実行されている SFIPS サーバだけが rsa-sha2-256 (SHA256WithRSA) をサポートします。</p> |
| SSH ホストキーアルゴリズム | <p>非推奨のアルゴリズム：</p> <ul style="list-style-type: none"> • ssh-rsa (SHA1withRSA) <p>新たにサポートされるアルゴリズム：</p> <ul style="list-style-type: none"> • rsa-sha2-256 • rsa-sha2-512 <p>(注) 14SU2以降のリリースにアップグレードする前に、『Cisco Unified Communications Manager および IM and Presence Service アップグレードおよび移行ガイド』の「COP ファイルでサポートされているアップグレードおよび移行パス」セクションを参照することをお勧めします。</p> |

| 特長 | 機能制限 |
|------------|--|
| IPSec ポリシー | <p>コモンクライテリア (CC) モードでは、証明書ベースの IPSec ポリシーの IPSec ポリシーを設定する前に、まずクラスタおよびノード間で証明書交換操作を行うことを推奨します。</p> <p>証明書ベースの IPSec ポリシーは、非 FIPS から FIPS およびコモンクライテリアモードに、またはその逆に移行すると機能しません。</p> <p>非 FIPS モードから FIPS および CC モードに、またはその逆に移行する必要がある場合は、次の手順を実行します。証明書ベースの IPSec ポリシーがあり、そのポリシーが有効な状態の場合：</p> <ol style="list-style-type: none"> 1. FIPS および CC モードに移行する前に IPSec ポリシーを無効にします。 2. 証明書を再認証し、FIPS および CC モードに移行した後、またはその逆に新しい証明書を交換します。 3. IPSec ポリシーを有効にします。 <p>(注) IPSec 構成を持つ FIPS CC モードサーバーを有効/無効にすると、複数の Pluto コアが表示されます (utils core active list)。ただし、これは機能上の影響はありません。</p> |

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 対応システムで稼働します。強化されたセキュリティ モードで動作するために、Unified Communications Manager と IM and Presence Service の両方を有効にすることで、次のセキュリティとリスク管理制御を備えるシステムを有効にすることができます。

- ユーザのパスワードとパスワードの変更に関して厳格化されたクレデンシャルポリシーが適用されます。
- デフォルトでは、連絡先検索の認証機能が有効です。
- リモート監査ログ用のプロトコルが TCP または UDP に設定されている場合は、デフォルトのプロトコルが 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。コモンクライテリアモードでは、厳密なホスト名検証が使用されます。そのため、証明書と一致する完全修飾ドメイン名 (FQDN) でサーバーを設定する必要があります。

Unified Communications Manager が FIPS モードの場合、バックアップデバイスとして設定するデバイスは FIPS 準拠である必要があります。キー交換アルゴリズム **diffie-hellman-group1-sha1** は FIPS モードではサポートされていません。非 FIPS モードの Unified Communications Manager

で **diffie-hellman-group1-sha1** アルゴリズムを設定すると、FIPS モードを有効にすると、このアルゴリズムは SSH キー交換から自動的に削除されます。

クレデンシャル ポリシーの更新

強化されたセキュリティモードを有効にすると、新しいユーザ パスワードとパスワード変更に関してより厳格なクレデンシャルポリシーが有効になります。強化されたセキュリティモードを有効にした後で、管理者は一連の CLI コマンド **set password ***** を使用して、次の要件のいずれかを変更できます。

- パスワードの長さは 14 ～ 127 文字です。
- パスワードには少なくとも 1 つの小文字、1 つの大文字、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。
- 過去 24 回以内に使用したパスワードを再使用することはできません。
- パスワードの最短有効期間は 1 日、最長有効期間は 60 日です。
- 新たに生成されるパスワードの文字列では、古いパスワードの文字列と少なくとも 4 文字が異なる必要があります。



(注) Unified Communications Manager と Cisco Instant and Messaging が拡張セキュリティモードで動作している場合、既存のローカルエンドユーザーまたは新しいローカルエンドユーザーで Jabber にログインする前に、ユーザーは次の手順に従う必要があります。

- まずセルフケアポータルにログインし、Jabber にログインする前にユーザーのパスワードをリセットします。次に、ローカルエンドユーザーの Jabber にログインします。
 - セルフケアポータルの URL : **https://<IPaddress>/ucmuser**
-



(注) Unified Communications Manager が拡張モードで動作できるようになっている場合は、IPMASysUser および IPMA SecureSysUser のユーザーログイン情報を変更してください。そうしないと、IPMA 機能は動作状態にならず、「IPMANotStarted」アラームがトリガーされます。CLI セッションは、次回の Cisco Tomcat サービスの再起動時または IPMA サービスの再起動時にフラッシュされます。

『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ログイン情報の管理」セクションに記載されているアプリケーションユーザーパスワードログイン情報を変更できます。

Cisco Unified CM Administration のユーザーインターフェイスから、[ユーザーの管理 (User Management)] > [アプリケーションユーザー (Application User)] に移動し、[ログイン情報の編集 (Edit Credential)] をクリックします。[認証ルール (Authentication Rule)] ドロップダウンリストから [強化されたセキュリティログイン情報ポリシー (Enhanced Security Credential Policy)] を選択し、[ユーザーは次回ログイン時に変更する必要があります (User Must Change at Next Login)] 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。「ログイン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。

強化されたセキュリティ モードの設定

強化されたセキュリティ モードを有効にする前に、FIPS を有効にしてください。

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、強化されたセキュリティモードを設定します。



(注) 拡張セキュリティモードを有効にした後で、Unified Communications Manager パブリッシュャのパスワードを変更する場合は、IM and Presence Service パブリッシュャのサービスが「STARTED」状態（「Cisco IM and Presence Data Monitor」サービスおよび SyncAgent）であることを確認する必要があります。

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、強化されたセキュリティモードが有効であるかどうかを確認します。

ステップ 3 Unified Communications Manager クラスタ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 モードを無効にするには、`utils EnhancedSecurityMode disable` コマンドを実行します。

ステップ 4 拡張セキュリティモードを有効にした後、Cisco Unified CM の管理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 パブリッシャで拡張セキュリティモードを有効にした後、次の手順を実行します。

1. Unified Communications Manager サブスクライバで拡張セキュリティモードを有効にします。
2. IM and Presence Service パブリッシャで拡張セキュリティモードを有効にします。
3. IM and Presence Service サブスクライバで拡張セキュリティモードを有効にします。

(注) **utils EnhancedSecurityMode enable** CLI コマンドまたは **utils EnhancedSecurityMode disable** CLI コマンドをすべてのノードで同時に実行しないでください。

コモンクライテリアモード

コモンクライテリアモードでは、Unified Communications Manager と IM and Presence Service サービスの両方がコモンクライテリアのガイドラインに準拠できます。コモンクライテリアモードは、各クラスタノードで次に示す CLI コマンドを使用して設定できます。

- ユーティリティ `fips_common_criteria` 有効
- ユーティリティ `fips_common_criteria disable`
- ユーティリティ `fips_common_criteria` ステータス

コモンクライテリア構成のタスクフロー

- 一般的な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 FIPS を有効にするよう求められます。FIPS を有効にすると、証明書を再生成する必要があります。詳細については、「[FIPS 140-2 モードの有効化 \(274 ページ\)](#)」を参照してください。
- コモンクライテリアモードでは、証明書ベースの IPSec ポリシーの IPSec ポリシーを設定する前に、クラスタおよびノード間で証明書交換操作が必須です。
- X.509 v3 証明書は、共通基準モードが必要です。X.509 v3 証明書は、次の通信プロトコルとして TLS 1.2 を使用する場合にセキュアな接続を有効にします。
 - リモート監査ログ
 - 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 をコモンクライトリアモードに設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---------------------------|---|
| ステップ 1 | TLSの有効化 (285 ページ) | TLS は、共通基準モードを設定するための前提条件です。 |
| ステップ 2 | コモンクライトリアモードの構成 (286 ページ) | Unified Communications Manager と IM and Presence Service のすべてのクラスタノードでコモンクライトリアモードを設定します。 |

TLSの有効化

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。TLS バージョン1.0 を使用したセキュア接続は、共通基準モードを有効にした後は許可されません。

- TLS 接続の確立中に、ピア証明書の `Extendedkeyusage` 拡張機能が適切な値についてチェックされます。
 - ピアがサーバの場合、ピア証明書には、 `Extendedkeyusage` 拡張機能として `serverauth` が必要です。
 - ピアがクライアントである場合、ピア証明書には、 `Extendedkeyusage` 拡張として `clientauth` が必要です。

`Extendedkeyusage` 拡張がピア証明書に存在しない場合、または正しく設定されていない場合は、接続が閉じられます。

TLS バージョン 1.2 をサポートするには、次の手順を実行します。

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 プラットフォームで実行している場合は、次のようにします。

- C:\Program Files\SmartBear\SoapUI-5.2.1\binに移動します。
-] `Vmoptions`] ファイルを編集して、追加-`dsoapui. https. プロトコル = tlsv 1.2, TLSv1, SSLv3`を編集し、ファイルを保存します。

ステップ 3 Linux で実行している場合は、 `bin/soapui. sh` ファイルを編集して `JAVA_OPTS = "$JAVA_OPTS-dsoapui. https. プロトコル = SSLv3, tlsv 1.2"` を追加し、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は、次のようになります。

- [アプリケーション (applications)]/[コンテンツ (Contents)] に移動します。
-] `Vmoptions`] を編集して、追加-`dsoapui. https. プロトコル = tlsv 1.2, TLSv1, SSLv3`を編集し、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。

コモンクライテリア モードの構成

Unified Communications Manager と IM and Presence Service サービスのコモンクライテリアモードを設定するには、次の手順を使用します。



(注) Cisco の CTL クライアントは、リリース 14 からサポートされなくなりました。Cisco CTL プラグインではなく、CLI コマンドを使用して、Unified Communications Manager サーバーを混合モードに切り替えることをお勧めします。

ステップ1 コマンドライン インターフェイス 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、システムがコモンクライテリアモードで実行されているかどうかを確認します。

ステップ3 クラスタ ノードで次のいずれかのコマンドを実行します。

- 共通基準モードを有効にするには、[コマンドユーティリティ (enable)] `fips_common_criteria` 実行します。
- 共通基準モードを無効にするには、[コマンドユーティリティ (disable)] `fips_common_criteria` 実行します。

共通基準モードが無効になっている場合は、最小 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) これらのコマンドをすべてのノードで同時に実行しないでください。

ステップ4 単一のクラスタ全体でコモンクライテリアモードを有効にするには、すべての Unified Communications Manager および 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 TLS 1.1 プロトコルと TLS 1.2 プロトコルをサポートしていないので、サーバがコモンクライテリアモードである場合、CTL クライアントは Unified Communications Manager ノードに接続しません。
 - 一般的な基準モードでは、TLS 1.1 または TLS 1.2 (DX シリーズおよび 88 XX シリーズの電話機など) をサポートする電話機モデルのみがサポートされています。7975 や 9971 などの TLSv 1.0 のみをサポートする電話機モデルは、共通基準モードではサポートされていません。
 - CTL クライアントを使用する際に一時的に TLS 1.0 を許可し、クラスタをコモンクライテリアモードに移します。最小 TLS を 1.1 または 1.2 に設定します。
 - コモンクライテリアモードで CLI コマンド `utils ctl set-cluster mixed-mode` を使用することにより、Tokenless CTL に移行します。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 がすでに設定されているマルチクラスタ設定で共通基準モードを有効にするには、次の順序で各ノードの共通基準モードを有効にします。

1. Unified Communications Manager - クラスタ 1 (パブリッシャ)
2. IM and Presence Service - クラスタ 1 (パブリッシャ)
3. IM and Presence Service - クラスタ 1 (1 つ以上のサブスクリバ)
4. Unified Communications Manager - クラスタ 2 (パブリッシャ)
5. IM and Presence Service - クラスタ 2 (パブリッシャ)
6. IM and Presence Service - クラスタ 2 (1 つ以上のサブスクリバ)

ステップ 6 証明書の同期に失敗した場合は、次を参照してください。



第 21 章

V.150 の最小必須要件

- [V.150 の概要 \(289 ページ\)](#)
- [V.150 設定のタスク フロー \(289 ページ\)](#)

V.150 の概要

「V.150 最低必須要件」機能を使用すると、IP ネットワーク経由のモデムで安全なコール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 勧告では、PSTN 上のモデムおよびテレフォニー デバイスと IP ネットワーク間でのモデム経由でのデータのリレー方法について、具体的に定義されています。V.150.1 は、ダイヤルアップ モデム コールをサポートしている IP ネットワークでのモデムの使用に関する ITU-T 勧告です。

Cisco V.150.1 Minimum Essential Requirements 機能は、国家安全保障局 (NSA) の SCIP-216 Minimum Essential Requirements (MER) for V.150.1 勧告の要件に準拠しています。SCIP-216 勧告により既存の V.150.1 要件が簡素化されました。

Cisco V.150.1 MER 機能は次のインターフェイスをサポートしています。

- Media Gateway Control Protocol (MGCP) T1 (PRI と 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 ポイント向けの Skinny Client Control Protocol (SCCP)
- Secure Communication Interoperability Protocol-End Instruments (SCIP-EI)

V.150 設定のタスク フロー

Unified Communications Manager に V.150 サポートを追加するには、次のタスクを完了します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | <p>メディア リソース グループ設定のタスク フロー (291 ページ) を行うには、次のサブタスクを実行します。</p> <ul style="list-style-type: none"> • 非 V.150 エンドポイントのメディア リソース グループの設定 (291 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 リストの設定 (292 ページ) • V.150 エンドポイントのメディア リソース グループの設定 (292 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 リストの設定 (293 ページ) | V.150 デバイスおよび非 V.150 デバイスのメディア リソース グループおよびメディア リソース グループ リストを追加します。 |
| ステップ 2 | Cisco V.150 (MER) に対応したゲートウェイの設定 (293 ページ) | ゲートウェイに V.150 機能を追加します。 |
| ステップ 3 | V.150 MGCP ゲートウェイ ポート インターフェイスの設定 (294 ページ) | MGCP ゲートウェイ全体で V.150 サポートを使用するには、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 インターフェイスの設定 (295 ページ) | SCCP ゲートウェイ全体で V.150 サポートを使用するには、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 | 電話での V.150 サポートの設定 (295 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 | <p>SIP トランク設定のタスク フロー (296 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。</p> <ul style="list-style-type: none"> • V.150 の SIP プロファイルの設定 (296 ページ) • クラスタ全体の V.150 フィルタの設定 (297 ページ) • SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加 (298 ページ) • V.150 の SIP トランクの設定 (298 ページ) | V.150 コールに使用する SIP トランクに V.150 サポートを追加します。 |
| 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ようにゲートウェイで 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 グループ設定のタスク フロー

システムですでに基本的なコール制御機能がセットアップされている必要があります。呼制御システムの設定方法については、『[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 の場合、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。

- 最小バージョンはリリース 10.5(2) SU3 です。
- 11.0 の場合、最小バージョンは 11.0(1) SU2 です。
- 11.5(1) 以降のすべてのリリースではこの機能がサポートされています。
- *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 を削除することが推奨されます。

2つのメディア リソース グループセット (非 V.150 コール用の MTP リソースからなるメディア リソースグループと、V.150 コール用の MTP リソースが含まれないメディア リソースグループ) を設定するには、次の作業を行います。

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 グループの設定 (291 ページ) | V.150 以外のエンドポイントに対して、MTP を使用してメディア 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 リストの設定 (292 ページ) | 非 V.150 エンドポイントの MTP メディア リソースが含まれているメディア リソース グループ リストを設定します。 |
| ステップ 3 | V.150 エンドポイントのメディア リソース グループの設定 (292 ページ) | セキュア V.150 コール用の MTP リソースが含まれていないメディア 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 リストの設定 (293 ページ) | セキュア V.150 エンドポイントに必要なリソースをメディア リソースグループに追加した後で、MTP のない非 V.150 エンドポイント用のメディア 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 グループの設定

非 V.150 エンドポイントの MTP リソースのメディア リソース グループを新たに追加するには、次の手順に従います。

-
- ステップ 1 Cisco Unified Communications Manager Administration から、[メディアリソース (Media Resources)] > [メディアリソースグループ (Media Resource Group)] を選択します。
- ステップ 2 [新規追加 (Add New)] 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名として「Do not use with V.150 devices」と入力します。
- 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 MTP デバイスだけを選択し、下矢印キーをクリックします。
選択したデバイスが [選択したメディアリソース (selected Media Resources)] 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の設定

[非 V.150 エンドポイントのメディアリソースグループの設定 \(291 ページ\)](#)

非 V.150 エンドポイントの MTP リソースのメディアリソースグループリストを新たに追加するには、次の手順に従います。

-
- ステップ 1 Cisco Unified Communications Manager Administration から、[メディアリソース (Media Resources)] > [メディアリソースグループリスト (Media Resource Group List)] を選択します。
- ステップ 2 [新規追加 (Add New)] 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として「Non- V.150」と入力します。
- 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、「Do not use with V.150 Devices」という名前の 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。
選択したデバイスが [選択したメディアリソース (selected Media Resources)] 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の設定

V.150 デバイスに対し、MTP リソースのない新しいメディアリソースグループを追加するには、次の手順に従います。

-
- ステップ 1 Cisco Unified Communications Manager Administration から、[メディアリソース (Media Resources)] > [メディアリソースグループ (Media Resource Group)] を選択します。
- ステップ 2 [新規追加 (Add New)] 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名として「For use with V.150 devices」と入力します。

- 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 MTP リソースを除く複数のデバイスを選択し、**下矢印キー**をクリックします。
選択したデバイスが **[選択したメディアリソース (selected Media Resources)]** 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 リストの設定

V.150 エンドポイントのメディア リソース グループの設定 (292 ページ)

V.150 デバイスの MTP リソースのメディア リソース グループ リストを追加するには、次の手順に従います。

- ステップ 1** Cisco Unified Communications Manager Administration から、**[メディアリソース (Media Resources)] > [メディアリソースグループリスト (Media Resource Group List)]** を選択します。
- ステップ 2** [新規追加 (Add New)] 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 リストの名前として **「V.150」** と入力します。
- 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)]** という名前の 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。
選択されたメディア リソース グループが **[Selected Media Resources]** 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 V.150 (MER) に対応したゲートウェイの設定

Cisco V.150 (MER) のゲートウェイを設定するには、次の手順を使用します。

- 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 (Add New)] をクリックします。
- ステップ 3** **[ゲートウェイタイプ (Gateway Type)]** 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** **[Protocol]** 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** ゲートウェイに対して選択するプロトコルに応じて、次のいずれかを実行します。
- MGCP の場合は、**[Domain Name]** 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 の場合は、**[MAC Address (Last 10 Characters)]** フィールドにゲートウェイ MAC アドレスを入力します。
- ステップ 7** **[Unified Communications Manager Group]** ドロップダウン リストから **[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。
- 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。
 - 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。
 - [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。各ポートアイコンは、ゲートウェイで利用可能なポートインターフェイスに対応します。対応するポートアイコンをクリックすることによって、任意のポートインターフェイスを設定できます。
- 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の設定

V.150 MGCP ゲートウェイポートインターフェイスを設定するには、次の手順を使用します。

- 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検索条件を入力し、[Find] をクリックします。
- ステップ 3** [設定されたスロット、VIC およびエンドポイント (Configured Slots, VICs, and Endpoints)] 領域で、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、該当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、[Next] をクリックします。
- (注) [Device Protocol] ドロップダウンリストが表示されるのは、[Configured Slots, VICs, and Endpoints] 領域で T1 ポートが選択されている場合だけです。
- [Gateway Configuration] ウィンドウにポート インターフェイス設定が表示されます。
- ステップ 5** 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 6** [V150 (subset)] チェックボックスをオンにします。
- 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) ゲートウェイで追加のポート インターフェイスを設定するには、[Related Links] ドロップダウン リストから [Back to MGCP Configuration] を選択し、[Go] をクリックします。異なるポートインターフェイスを選択できます。

V.150 SCCP ゲートウェイ ポート インターフェイスの設定

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には、次の手順を使用します。

- 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 SCCP ゲートウェイの設定を変更するための検索条件を入力し、[Find] をクリックします。
- ステップ 3 [設定されたスロット、VIC およびエンドポイント (Configured Slots, VICs, and Endpoints)] 領域で、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、該当するポートアイコンをクリックします。
- ステップ 4 「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 5 [Product Specific Configuration Layout] 領域で [Latent Capability Registration Setting] ドロップダウンリストが表示される場合は、[Modem Relay] または [Modem Relay and Passthrough] を選択します。
- 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。

電話での V.150 サポートの設定

電話に V.150 のサポートを追加するには、次の手順を使用します。V.150 をサポートする電話のタイプは次のとおりです。

- Cisco 7962 : Cisco 7962 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
- 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

- ステップ 1 必須: 目的の電話番号と同じユーザ ID を使用して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 エンドポイントの [エンドユーザ設定 (End User Configuration)] ウィンドウの [ダイジェストログイン情報 (Digest Credentials)] フィールドを設定します。
新しいエンドユーザーの設定方法の詳細については、『[Cisco Unified Communications Manager システム設定ガイド](#)』の「[エンドユーザーの手動プロビジョニング]」の章を参照してください。
- ステップ 3 Cisco Unified Communications Manager Administration から、[デバイス (Device)] > [電話 (Phone)] 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。
 - 既存の電話で V.150 を設定するには、[検索 (Find)] をクリックして電話を選択します。
 - 新しい電話で V.150 を設定するには、[新規追加 (Add New)] をクリックします。

- ステップ 5** [電話のタイプ (Phone Type)] ドロップダウンリストから、V.150 をサポートする電話のタイプを選択し、[次へ (Next)] をクリックします。
- ステップ 6** Cisco 7962 として登録されたサードパーティの SCCP エンドポイントの場合は、[デバイスプロトコル (Device Protocol)] ドロップダウンリストから [SCCP] を選択し、[次へ (Next)] をクリックします。
- ステップ 7** [Media Resource Group List] 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** サードパーティの AS-SIP SIP エンドポイントの場合のみ、次のフィールドを設定します。
- [Digest User] 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。このエンドユーザがダイジェスト認証に使用されます。
 - [メディアターミネーションポイント必須 (Media Termination Point Required)] チェックボックスはオフのままにします。
 - [音声とビデオ コールの Early Offer サポート (Early Offer support for voice and video calls)] チェックボックスをオンにします。
- 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 トランク設定のタスク フロー

SIP トランクタスクフローを設定するには、次の手順を使用します。

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 プロファイルで SIP トランクの SIP Best Effort Early Offer サポートを設定します。 |
| ステップ 2 | クラスタ全体の V.150 フィルタの設定 (297 ページ) | オプション。クラスタ全体での SIP V.150 SDP オファァー フィルタリングのデフォルト設定を行います。 |
| ステップ 3 | SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加 (298 ページ) | 特定の SIP トランクに割り当て可能な SIP トランク セキュリティプロファイル内で V.150 フィルタを設定します。 |
| ステップ 4 | V.150 の SIP トランクの設定 (298 ページ) | V.150 コールを処理する SIP トランクで V.150 サポートを設定します。 |

V.150 の SIP プロファイルの設定

SIP プロファイルで SIP トランクの SIP Best Effort Early Offer サポートを設定するには、次の手順を実行します。

-
- ステップ 1** Cisco Unified Communications Manager Administrationで、[デバイス (Device)] > [デバイスの設定 (Device Settings)] > [SIP プロファイル (SIP 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。
- 新しいプロファイルを作成するには、[Add New] 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 (Find)] 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(Name)] 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、V.150 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 [Select Best Effort (no MTP inserted)] を選択します。
- ステップ 6** 必要なその他の設定値を入力します。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。
-

クラスタ全体の V.150 フィルタの設定

クラスタ全体での SIP V.150 SDP オファー フィルタリングのデフォルト設定には、次の手順を使用します。



- (注) SIP トランク セキュリティ プロファイル内の [SIP V.150 SDP Offer Filtering] 値に、クラスタ全体のサービス パラメータ設定とは異なる値を設定すると、このセキュリティプロファイル設定により、そのセキュリティプロファイルを使用するトランクのクラスタ全体のサービス パラメータ設定がオーバーライドされます。
-

- ステップ 1** Cisco Unified Communications Manager Administrationから、[System (システム)] > [Service Parameters (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** [Clusterwide Parameters (Device- SIP)] セクションで [SIP V.150 SDP Offer Filtering] サービス パラメータの値を設定します。
- ステップ 5** ドロップダウン リストから [SIP V.150 SDP Offer Filtering] を選択します。
- ステップ 6** 目的の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。
-

SIP トランク セキュリティ プロファイルへの V.150 フィルタの追加

SIP トランク セキュリティ プロファイル内で V.150 フィルタを割り当てるには、次の手順を実行します。



- (注) SIP トランク セキュリティ プロファイルの [SIP V.150 SDP Offer Filtering] に、クラスタ全体のサービスパラメータとは異なる値を設定すると、このセキュリティ プロファイル設定は、そのセキュリティ プロファイルを使用するトランクのクラスタ全体のサービスパラメータ設定をオーバーライドします。

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)] > [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 次のいずれかの操作を行います。

- 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するには、検索条件を入力して [検索 (Find)] をクリックし、リストから既存のプロファイルを選択します。
- 新しい SIP トランク セキュリティ プロファイルを追加するには、[新規追加 (Add New)] をクリックします。

ステップ 3 [SIP V.150 SDP Offer Filtering] 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、クラスタ全体のサービスパラメータ [SIP V.150 Outbound SDP Offer Filtering] の値が使用されます。

ステップ 4 [SIP Trunk Security Profile Configuration] ウィンドウのその他のフィールドをすべて設定します。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 5 [保存 (Save)] をクリックします。

V.150 の SIP トランクの設定

SIP トランクの設定を行うには、次の手順に従います。

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 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、[Add New] をクリックします。
- 既存のトランクを選択するには、[検索 (Find)] をクリックして 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は次の手順に従います。

- [Trunk Type] ドロップダウン リストから [SIP Trunk] を選択します。

- **[Protocol Type]** ドロップダウンリストから、**[SIP]** を選択します。
- **[Trunk Service Type]** ドロップダウンリストから **[None(Default)]** を選択します。
- **[次へ (Next)]** をクリックします。

- ステップ 4** [名前(Name)] 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(Description)] 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** **[Media Resource Group List]** 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 **[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、**[+]** ボタンをクリックします。SIP トランクには最大 16 個の宛先を追加できます。
- ステップ 8** **[SIP Trunk Security Profile]** ドロップダウンリストから、このトランクに設定した SIP トランク セキュリティ プロファイルを割り当てます。
- ステップ 9** **[SIP Profile]** ドロップダウンリストから、**[Best Effort Early Offer]** 設定でセットアップした SIP プロファイルを割り当てます。
- ステップ 10** **[Media Termination Point Required]** チェックボックスはオフのままにします。
- 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 の設定

- [IPsec の概要 \(301 ページ\)](#)

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の IPSec 設定

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 を設定する際の考慮事項と推奨事項について記載されています。IPsec をネットワーク インフラストラクチャで設定し、Unified Communications Manager とデバイスとの間では設定しない場合は、IPsec の設定前に、次のことを検討してください。

- IPsec は、Unified Communications Manager 自体ではなく、インフラストラクチャで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 接続または VPN 接続、プラットフォームの CPU への影響、帯域幅への影響、ジッターや遅延などの評価指標について考慮します。
- 『*Voice and Video Enabled IPsec Virtual Private Networks Solution Reference Network Design Guide*』を参照します。
- 『*Cisco IOS Security Configuration Guide, Release 12.2*』 (またはそれ以降) を参照します。
- IPsec 接続のリモートエンドをセキュアな CiscoIOS MGCP ゲートウェイで終端します。
- テレフォニーサーバが存在するネットワークの信頼された球体内のネットワークデバイスでホストの終端を終端します。たとえば、ファイアウォール、アクセスコントロールリスト (ACL)、またはその他のレイヤ3デバイスの背後にあります。

- ホスト側 IPsec 接続の終端に使用する機器は、ゲートウェイの数とそれらのゲートウェイに予想されるコールの量とによって決まります。たとえば、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、Cisco サービス統合型ルータなどがあります。
- セキュアゲートウェイとトランクの設定に関連するトピックで指定されている順序で手順を実行します。



注意 IPsec 接続を設定してその接続がアクティブであることを確認しないと、メディアストリームのプライバシーが損なわ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の間で IPsec セットアップを構成および管理する

説明されている Unified Communications Manager とゲートウェイまたはトランク間での 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」を参照してください。



第 23 章

CTI、JTAPI、および TAPI の認証および暗号化の設定

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の概要について説明します。また、CTI、TAPI、および JTAPI アプリケーションの認証と暗号化の設定のため、[Unified Communications Manager Administration] で実行する必要がある作業についても説明します。

このドキュメントでは、[Unified Communications Manager Administration] で使用可能な Cisco JTAPI や TSP プラグインのインストール方法は説明しません。また、インストール中にセキュリティパラメータを設定する方法についても説明しません。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ません。

- [CTI、JTAPI、および TAPI アプリケーションの認証 \(303 ページ\)](#)
- [CTI、JTAPI、および TAPI アプリケーションの暗号化 \(305 ページ\)](#)
- [CTI、JTAPI、および TAPI アプリケーションの CAPF の機能 \(307 ページ\)](#)
- [CTI、JTAPI、および TAPI の保護 \(314 ページ\)](#)
- [セキュリティ関連のアクセス制御グループへのアプリケーションとエンドユーザの追加 \(315 ページ\)](#)
- [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 \(317 ページ\)](#)
- [アプリケーションまたはエンドユーザの証明書の操作ステータスの表示 \(318 ページ\)](#)

CTI、JTAPI、および TAPI アプリケーションの認証

Unified Communications Manager を使用して、CTIManager と CTI/JTAPI/TAPI アプリケーションとの間のシグナリング接続およびメディアストリームを保護できます。



(注) Cisco JTAPI/TSP プラグインのインストール中に、セキュリティ設定を構成したとします。また、Cisco CTL クライアント、または CLI コマンドセットの **utils ctl** で、クラスタ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も前提としています。この章で説明する作業を実行する際に、これらの設定が定義されていない場合、CTIManager とアプリケーションは非セキュアポートのポート 2748 で接続されます。

Cisco の CTL クライアントは、リリース 14 からサポートされなくなりました。Cisco CTL プラグインではなく、CLI コマンドを使用して、Unified Communications Manager サーバーを混合モードに切り替えることをお勧めします。

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) によって他方の当事者の id を確認します。TLS 接続が確立されると、CTIManager およびアプリケーションでは、TLS ポートのポート 2749 を介して QBE メッセージを交換します。

アプリケーションとの認証を行うために、CTIManager は、Unified Communications Manager 証明書 (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、またはプラットフォームにアップロードされたサードパーティの CA 署名付き証明書) を使用します。

CLI コマンドセットの **monitorctl** または Cisco **ctl** クライアントを使用して **ctl** ファイルを生成した後、この証明書は **ctl** ファイルに自動的に追加されます。アプリケーションでは、CTL ファイルを TFTP サーバからダウンロードした後で、CTIManager への接続を試みます。

JTAPI/TSP クライアントが最初に TFTP サーバから CTL ファイルをダウンロードするときに、JTAPI/TSP クライアントは CTL ファイルを信頼します。JTAPI/TSP クライアントでは CTL ファイルを検証しないため、このダウンロードはセキュアな環境で実行することを推奨します。JTAPI/TSP クライアントは、その後の 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。ファイルの内容には、Unified Communications Manager 証明書と CAPF サーバ証明書が含まれます。

CTL ファイルが侵害された場合、JTAPI/TSP クライアントはダウンロードした 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 ファイル内の古い証明書を使用して TLS 接続を確立しようとします。CTL ファイルが変更されたか、または侵害された場合、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、複数の TFTP サーバが存在する場合は、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。

- クライアントは何らかの理由で CTL ファイルをダウンロードできません。たとえば、CTL ファイルは存在しません。
- クライアントには、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 ユーザとして設定しました。

アプリケーションは、CTIManager を使用して認証するために、認証局プロキシ機能 (CAPF) によって発行される証明書を使用します。アプリケーションと CTIManager との間のすべての

接続で TLS を使用するには、アプリケーションの PC で実行されているインスタンスごとに一意の証明書が必要です。1つの証明書がすべてのインスタンスをカバーしていません。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インストールされるようにするには、「CAPF の設定項目」の説明に従って、Cisco Unified Communications Manager Administration で、それぞれの [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)] または [エンドユーザ CAPF プロファイルの設定 (End User CAPF Profile Configuration)] に一意のインスタンス ID を設定します。



ヒント アプリケーションをある PC から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 のインスタンスごとに新しい証明書をインストールする必要があります。

また、アプリケーションの TLS を有効にするには、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 Standard CTI Secure Connection ユーザグループに追加する必要があります。このグループにユーザを追加して証明書をインストールすると、アプリケーションによって、ユーザが TLS ポート経由で接続することが保証されます。

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ません。CTIManager サービスに接続する CTI クライアントでは、クライアントが音声パケットを送信する場合、暗号化がサポートされることがあります。

アプリケーションと CTIManager 間のメディアストリームを保護するには、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 SRTP キー情報の受信許可 (Standard CTI Allow Reception of SRTP Key Material)] ユーザグループに追加します。これらのユーザが Standard CTI Secure Connection 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になっている場合、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主要な資料を提供します。



(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能力を設定します。

アプリケーションは SRTP キー資料を記録したり保存したりしませんが、アプリケーションはキーマテリアルを使用して RTP ストリームを暗号化し、CTIManager から SRTP ストリームを復号化します。

アプリケーションが非セキュアポートであるポート 2748 に何らかの理由で接続されると、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 がデバイスまたは電話番号をモニタ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が、Standard CTI Enabled、Standard CTI Secure Connection、および Standard CTI で SRTP キー情報の受信を許可する3つのグループに存在する必要があります。

Unified Communications Managerは、CTIports およびルートポイントで送受信されるセキュアコールを円滑にしますが、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、セキュア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。

CTIports/ルートポイントは、ダイナミックまたはスタティック登録によって登録します。ポート/ルートポイントがダイナミック登録を使用している場合、各コールに対してメディアパラメータが指定されます。スタティック登録の場合、メディアパラメータは登録時に指定され、コール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、デバイスはセキュアに登録され、アプリケーションがデバイス登録要求で有効な暗号化アルゴリズムを使用し、他方がセキュアである場合は、SRTP を介してメディアが暗号化されます。

CTI アプリケーションがすでに確立されているコールのモニタリングを開始すると、アプリケーションは RTP イベントを受信しません。確立されたコールの場合、CTI アプリケーションは DeviceSnapshot イベントを提供します。これは、コール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、キー素材を提供しません。

CTI ポートの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、デバイスはセキュアに登録され、アプリケーションがデバイス登録要求で有効な暗号化アルゴリズムを使用し、他方がセキュアである場合は、Secure Real-Time Transport Protocol (SRTP) を介してメディアが暗号化されます。

Unified Communications Manager は、CTI ポートの Skinny Client Control Protocol (SCCP) インターフェイスに強力な暗号スイートを提供し、発信側と着信側間のセキュア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 を提供することによって登録します。

Unified Communications Manager は、CTI ポートを含むセキュアコールで次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拡張されています。

- 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)

コールを受信すると、Unified Communications Manager は、CTI アプリケーションで指定されたメディアおよび暗号化機能をネゴシエートし、着信側の電話機の 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 は両側にキー情報を送信してパケットを復号化し、メディアをモニタまたは記録します。

制限

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を使用して CTI ポート終端メディアを登録しようとすると、Unified CM はそれを無視し、使用可能な残りのアルゴリズムのうち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 はデフォルトで既存の動作に切り替え、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 の機能

認証局プロキシ機能 (CAPF) は Unified Communications Manager とともに自動的にインストールされ、設定に応じて次の CTI/TAPI/TAPI アプリケーション用のタスクを実行します。

- 認証文字列を使用して JTAPI/TSP クライアントに対して認証を行う。
- CTI/JTAPI/TAPI アプリケーションユーザまたはエンドユーザにローカルで有効な証明書 (LSC) を発行する。
- 既存のローカルで有効な証明書をアップグレードする。
- 表示やトラブルシューティングのために証明書を取得する。

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 に認証されます。その後、クライアントが公開キーと秘密キーのペアを生成し、署名付きメッセージによって公開キーを CAPF サーバに転送します。秘密キーはクライアントに残り、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クライアントに送り返されます。

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、[Application User CAPF Profile Configuration] ウィンドウまたは [End User CAPF Profile Configuration] ウィンドウでそれぞれ設定を行います。次に、Unified Communications Manager がサポートする CAPF プロファイルの違いについて説明します。

- **アプリケーションユーザ CAPF プロファイル**：このプロファイルでは、CTIManager サービスとアプリケーションの間で TLS 接続をオープンできるようにするため、セキュアなアプリケーションユーザに対してローカルで有効な証明書を発行できます。

1つのアプリケーションユーザ CAPF プロファイルが、サーバのサービスまたはアプリケーションの1つのインスタンスに対応します。同じサーバで複数の Web サービスやアプリケーションをアクティブにする場合は、サーバのサービスごとに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台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ブにする場合、サーバごとに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**：このプロファイルでは、CTI クライアントが TLS 接続を介して CTIManager サービスと通信できるよう、CTI クライアントに対してローカルで有効な証明書を発行できます。



ヒント JTAPI クライアントは、[JTAPI Preferences] ウィンドウで設定したパスに、Java キーストア形式で LSC を保存します。TSP クライアントは、デフォルトディレクトリまたは設定したパスに、暗号化された形式で LSC を保存します。

次の情報は、通信または電源障害が発生した場合に適用されます。

- 証明書のインストールが行われている間に通信障害が発生した場合、JTAPI クライアントは証明書の取得を30秒間隔でさらに3回試行します。この値は設定できません。

TSP クライアントでは、再試行回数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に証明書を取得しようとする回数を指定して、これらの値を設定します。両方の値について、デフォルトは0です。1 (1回の再試行)、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。再試行ごとに30秒以内に設定できます。

- JTAPI/TSP クライアントが CAPF とのセッションを試行している間に電源障害が発生した場合、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行します。

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

CAPF には次の要件があります。

- アプリケーションユーザとエンドユーザの 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 (Enterprise Parameters Configuration)] ウィンドウの [クラスタセキュリティモード (Cluster Security Mode)] を 1 (混合モード) に設定します。
- 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アクティブにする必要があります。
- 多くの証明書を同時に生成するとコールプロセス中断の原因となるため、スケジュールされたメンテナンスの時間帯に CAPF を使用することを推奨します。

- 証明書操作の全期間を通じて、パブリッシャノードが正常に実行されていることを確認します。
- 証明書の操作全体で CTI/JTAPI/TAPI アプリケーションが機能していることを確認します。

Certificate Authority Proxy Function サービスのアクティブ化

Unified Communications Manager は、Cisco Unified Serviceability で認証局プロキシ機能サービスを自動的にアクティブ化しません。

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ブにする必要があります。

Unified Communications Manager を混合モードに移行する前にこのサービスをアクティブにしなかった場合は、CTL ファイルを更新する必要があります。

Cisco Certificate Authority Proxy Function サービスをアクティブにすると、CAPF 固有のキーペアおよび証明書が CAPF によって自動的に生成されます。CAPF 証明書は、CAPF 証明書が存在することを検証として、Cisco Unified Communications オペレーティングシステムの 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 プロファイルの設定

JTAPI/TAPI/CTI アプリケーション用の重要な証明書をローカルでインストール/アップグレード/トラブルシューティングする場合は、「[CAPF の設定項目](#)」を参考にしてください。



ヒント アプリケーションユーザ CAPF プロファイルを設定してからエンドユーザ CAPF プロファイルを設定することを推奨します。

- ステップ 1** Cisco Unified Communications Manager Administration で、次のいずれかのオプションを選択します。
- a) [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [アプリケーションユーザ CAPF プロファイル (Application User CAPF Profile)]
 - b) [ユーザ管理 (User Management)] > [ユーザ設定 (User Settings)] > [エンドユーザ CAPF プロファイル (End User CAPF Profile)]
- ステップ 2** 次のいずれかの操作を行います。
- a) 既存のプロファイルを編集するには、[検索 (Find)] をクリックし、既存のプロファイルを編集します。
 - b) 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。
 - c) 既存のプロファイルから新しいプロファイルに設定をコピーするには、[検索 (Find)] をクリックし、目的の設定がある既存のプロファイルを選択します。[コピー (Copy)] をクリックして、それらの設定を含む新しいプロファイルに名前を付けます。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** 「[CAPF の設定項目](#)」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。

ステップ5 この手順を繰り返して、さらに CAPF プロファイルを作成します。ユーザに必要な数のプロファイルを作成します。

[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)] ウィンドウで **CCMQRTSecureSysUser**、**IPMAMSecureSysUser**、または **WDSecureSysUser** を設定した場合は、**サービスパラメータ**を設定する必要があります。

CAPF の設定項目

次の表で、[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)] および [エンドユーザ CAPF プロファイルの設定 (End User CAPF Profile Configuration)] ウィンドウの CAPF の設定項目について説明します。

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)] | <p>ドロップダウンリストから、CAPF 操作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。</p> <p>この設定は、[エンドユーザ CAPF プロファイル (End User CAPF Profile Configuration)] ウィンドウには表示されません。</p> |
| [エンドユーザ ID (End User ID)] | <p>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。この設定は設定済みのエンドユーザを示します。</p> <p>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 Configuration)] ウィンドウには表示されません。</p> |
| [インスタンス ID (Instance ID)] | <p>1 ~ 128 文字の英数字 (a ~ z、A ~ Z、0 ~ 9) を入力します。インスタンス ID は、証明書を操作するユーザを識別します。</p> <p>アプリケーションの複数の接続先 (インスタンス) を設定できます。アプリケーションと CTIManager 間の接続を保護するには、アプリケーション PC (エンドユーザ用) またはサーバ (アプリケーションユーザ用) 上で実行される各インスタンスが固有の証明書を持っていることを確認します。</p> <p>このフィールドは、Web サービスと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ます。</p> |

| 設定 | 説明 |
|------------------------------------|--|
| [証明書 の操作 (Certificate Operation)] | <p>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。</p> <ul style="list-style-type: none"> • [保留中の操作なし (No Pending Operation)] : 証明書の操作が発生しない場合に表示されます。(デフォルト設定) • [インストール/アップグレード (Install/Upgrade)] : アプリケーションに新しい証明書をインストールするか、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。 |
| [認証モード (Authentication Mode)] | <p>証明書の操作が [インストール/アップグレード (Install/Upgrade)] の場合、認証モードとして [認証文字列 (By Authentication String)] が指定されます。つまり、ユーザ/管理者によって [JTAPI/TSP 設定 (JTAPI/TSP Preferences)] ウィンドウに CAPF 認証文字列が入力された場合にのみ、ローカルで有効な証明書のインストール/アップグレードまたはトラブルシューティングが CAPF によって実行されます。</p> |
| [認証文字列 (Authentication String)] | <p>手動で一意的な文字列を入力するか、[文字列の生成 (Generate String)] ボタンをクリックして文字列を生成します。</p> <p>4 桁から 10 桁の文字列が含まれていることを確認します。</p> <p>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必要があります。この文字列は、1 回の使用のみをサポートしており、文字列をインスタンスで使用した後は、再び使用できません。</p> |
| [文字列の生成 (Generate String)] | <p>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 (Generate String)] ボタンをクリックします。[認証文字列 (Authentication String)] フィールドに 4 桁から 10 桁の認証文字列が表示されます。</p> |

| 設定 | 説明 |
|---|--|
| [キーの順序 (Key Order)] | <p>このフィールドは、CAPF のキーの順序を指定します。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。</p> <ul style="list-style-type: none"> • [RSA のみ (RSA Only)] • [ECのみ (EC Only)] • [EC 優先、RSA バックアップ (EC Preferred, RSA Backup)] <p>(注) [キーの順序 (Key Order)]、[RSAキーサイズ (RSA Key Size)]、および[ECキーサイズ (EC Key Size)]の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 プロファイルはその電話に関連付けられます。値 [ECのみ (EC Only)]と [ECキーサイズ (EC Key Size)]で256ビットの値を選択した場合、デバイスセキュリティ プロファイルには [EC-256] の値が追加されます。</p> |
| [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) (EC Key Size (Bits))] | 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。 |
| [操作完了期限 (Operation Completes by)] | <p>このフィールドは操作を完了する必要がある期限の日時を指定します。このフィールドはすべての証明書操作に対応しています。</p> <p>表示される値は、最初のノードに適用されます。</p> <p>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アップデートできます。</p> |
| [証明書の操作ステータス (Certificate Operation Status)] | <p>このフィールドには、保留中、失敗、成功といった証明書の操作の進行状況が表示されます。</p> <p>このフィールドに表示される情報は変更できません。</p> |

CAPF サービス パラメータの更新

[サービスパラメータ (Service Parameter)] ウィンドウには、Cisco Certificate Authority Proxy Function のオプション設定があります。CAPF 証明書の証明書発行者、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。

Cisco Unified Communications Manager Administration で CAPF サービスパラメータをアクティブとして表示するには、Cisco Unified Serviceability で[認証局プロキシ機能 (Certificate Authority Proxy Function)] サービスを有効にします。



ヒント 電話機に 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、次の手順を実行します。

ステップ 1 Cisco Unified Communications Manager Administration から、[**System (システム)**] > [**Service Parameters (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 クラスタ内のパブリッシュャ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で、[**Cisco Certificate Authority Proxy Function**] サービスを選択します。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 オンラインヘルプの説明に従って、**CAPF サービスパラメータ**を更新します。**CAPF 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リンクをクリックします。

ステップ 5 変更内容を有効にするには、Cisco Unified Serviceability で、**Cisco Certificate Authority Proxy Function** サービスを再起動します。

(注) 認証局プロキシ機能の設定方法の詳細については、「**認証局プロキシ機能**」の章を参照してください。

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

Cisco Unified Communications Manager Administration で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、該当プロファイルを使用するすべてのデバイスを削除してください。プロファイルを使用してい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)] ウィンドウの [関連リンク (Related Links)] ドロップダウンリストで [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。

依存関係レコード機能がシステムで有効でない場合は、依存関係レコード概要ウィンドウに、依存関係レコードを有効にするために実行できる操作が表示されます。また、依存関係レコード機能に関連して CPU 負荷が高くなることについての情報も表示されます。依存関係レコードの詳細については、『[Cisco Unified Communications Manager システム設定ガイド](#)』を参照してください。

ここでは、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を説明します。

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 プロファイルを検索します。

ステップ 2 次のいずれかの操作を行います。

- a) 複数のプロファイルを削除するには、[**Find And List**] ウィンドウの該当するチェックボックスの横にあるチェックボックスをオンにします。次に、[**Delete Selected**] をクリックします。この選択で設定可能なすべてのレコードを削除するには、[すべて選択 (Select All)] をクリックして、[選択項目の削除 (Delete Selected)] をクリックします。
- b) 1つのプロファイルを削除するには、[**Find And List**] ウィンドウで該当するプロファイルの横にあるチェックボックスをオンにします。次に、[**Delete Selected**] をクリックします。

ステップ 3 削除操作を確認するプロンプトが表示されたら、[OK] をクリックして削除するか、[Cancel] をクリックして削除の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について説明します。

ステップ 1 CTI アプリケーションと JTAPI/TSP プラグインがインストールされ、実行されていることを確認します。

ヒント アプリケーションユーザを Standard CTI Enabled グループに割り当てます。

詳細については、次の資料を参照してください。

- *Unified Communications Manager* の *Cisco JTAPI* インストールガイド
- *Unified Communications Manager* の *Cisco TAPI* インストールガイド

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ます（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）。

- `utlis ctl` コマンドセットを実行して、Unified Communications Manager が混合モードになっているかどうかを確認します。
- CAPF サービスがインストールされ、サービスがアクティブ化され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、CTL ファイルに CAPF 証明書を含めるために、`utils ctl` CLI コマンドに対して実行する必要があります。電話機に 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、パラメータを再度更新する必要はありません。

- クラスタ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。）

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制御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ます。これにより、ユーザは CTI 接続で **TLS** および **SRTP** を使用できます。

- 標準 CTI 対応
- 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またはエンドユーザのいずれかに割り当てることができますが、両方に割り当てることはできません。

ユーザはすでに **Standard CTI Enabled** および **Standard CTI Secure Connection** ユーザグループ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つのグループに存在しない場合、SRTPセッションキーを受信できません。詳細については、ユーザアクセス制御グループの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ません。CTIManager サービスに接続する CTI クライアントでは、クライアントが音声パケットを送信する場合、暗号化がサポートされることがあります。

ステップ 4 エンドユーザと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。詳細については、「**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 アプリケーションで、対応するセキュリティ関連のパラメータを有効にします。

セキュリティ関連のアクセス制御グループへのアプリケーションとエンドユーザの追加

Standard CTI Secure Connection ユーザグループおよび Standard CTI Allow Reception of SRTP Key Material ユーザグループは、デフォルトで Unified Communications Manager に表示されます。これらのグループは削除できません。

CTIManager へのユーザ接続を保護するには、[Standard CTI Secure Connection] ユーザグループにアプリケーションユーザまたはエンドユーザを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またはエンドユーザのいずれかに割り当てることができますが、両方に割り当てることはできません。

アプリケーションと CTIManager でメディアストリームを保護する場合は、アプリケーションユーザまたはエンドユーザを Standard CTI Allow Reception of SRTP Key Material 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 を使用できるようになるには、そのユーザは、TLS のベースライン設定として機能する Standard CTI Enabled および Standard CTI Secure Connection ユーザグループに存在している必要があります。SRTP 接続には TLS が必要です。ユーザがこれらのグループに存在する場合は、標準 CTI にユーザを追加して、SRTP キーマテリアルユーザグループの受信を許可することができます。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が、**Standard CTI Enabled**、**Standard CTI Secure Connection**、および **Standard CTI** で **SRTP キー情報の受信を許可する**3つのグループに存在している必要があります。

Cisco Unified Communications Manager Assistant、CiscoQRT、および Cisco Web Dialer が暗号化をサポートしていないため、アプリケーションユーザ (CCMQRTSecureSysUser、IPMA SecureSysUser、および WDSecureSysUser) を標準 CTI SRTP 重要素材の受信許可ユーザグループに追加する必要はありません。



ヒント ユーザグループからのアプリケーションユーザ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。[**ロールの設定 (Role Configuration)**] ウィンドウで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。

- ステップ 1** Cisco Unified Communications Manager Administration から、[**ユーザ管理 (User Management)**] > [**ユーザグループ (User Group)**] 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 (Find)**] をクリックします。
- ステップ 3** 実行する内容に応じて、次のいずれかの作業を行います。
- アプリケーションまたはエンドユーザが Standard CTI Enabled グループに存在することを確認します。
 - Standard CTI Secure Connection** ユーザグループにアプリケーションユーザまたはエンドユーザを追加するには、[**標準 CTI セキュア接続 (Standard CTI Secure Connection)**] リンクをクリックします。
 - Standard CTI Allow Reception of SRTP Key Material** ユーザグループにアプリケーションユーザまたはエンドユーザを追加するには、[**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** アプリケーション ユーザをグループに追加するには、手順 5~7 を実行します。
- ステップ 5** [グループにアプリケーションユーザを追加 (Add Application Users to Group)] をクリックします。
- ステップ 6** アプリケーションユーザを検索するには、検索条件を指定します。次に、[**検索 (Find)**] をクリックします。
- 検索条件を指定せずに [検索 (Find)] をクリックすると、使用可能なすべてのオプションが
- ステップ 7** グループに追加するアプリケーション ユーザのチェックボックス (複数可) をオンにし、[Add Selected] をクリックします。
- ユーザが [ユーザグループ (User Group)] ウィンドウに表示されます。
- ステップ 8** エンドユーザをグループに追加するには、ステップ 9~11 を実行します。
- ステップ 9** [グループにユーザを追加 (Add Users to Group)] をクリックします。

- ステップ 10** エンドユーザを検索するには、検索条件を指定します。次に、**[検索 (Find)]** をクリックします。
検索条件を指定せずに **[Find]** をクリックすると、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のチェックボックス（複数可）をオンにし、**[Add Selected]** をクリックします。
ユーザが **[ユーザグループ (User Group)]** 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

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 プロファイルを設定した後、**Cisco IP Manager Assistant** サービスに対して、次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
- CAPF Profile Instance ID for Secure Connection to CTIManager

サービスパラメータにアクセスするには、次の手順を実行します。

- ステップ 1** Cisco Unified Communications Manager Administration から、**[System (システム)] > [Service Parameters (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、**[Cisco IP Manager Assistant]** サービスがアクティブになっている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 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]** パラメータおよび **[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** 疑問符またはパラメータ名のリンクをクリックしたときに表示されるヘルプの説明に従って、パラメータを更新します。
- ステップ 6** **[保存 (Save)]** をクリックします。
- ステップ 7** サービスがアクティブになっているサーバごとに、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の操作ステータスの表示

特定の [アプリケーションユーザ CAPF プロファイル設定 (Application User CAPF Profile configuration)] または [エンドユーザ CAPF プロファイル設定 (End User CAPF Profile configuration)] ウィンドウで、または ([検索/一覧表示 (Find/List)] ウィンドウではなく) [JTAPI/TSP 設定 (JTAPI/TSP Preferences)] GUI ウィンドウで、証明書操作ステータスを確認できます。



第 24 章

セキュアな録音とモニタリング

- [セキュアコールのモニタリングと録音のセットアップについて \(319 ページ\)](#)
- [セキュアなコールのモニタリングと録音のセットアップ \(320 ページ\)](#)

セキュアコールのモニタリングと録音のセットアップについて

セキュア コールは、この項で説明するようにモニタリングおよび録音を行えます。

- セキュリティ保護された、またはセキュリティ保護されていないコールに対して、セキュリティ保護されたモニタリングセッションを確立できます。
- コールモニタリング要求の結果として、元のコールのコールセキュリティが影響を受けたり、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機能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、続行が許可されます。
- エージェントとカスタマー間の元のコールには、モニタリングコールとは異なる暗号キーが必要です。モニタリングセッションでは、システムはエージェントと顧客の混合音声を、最初に新しいキーを使用して暗号化してから、上司に送信します。



- (注) Unified Communications Manager は、安全でないレコーダを使用中に、認証済みコールのコール録音をサポートします。セキュアコールレコーダを使用したコールの場合、レコーダが SRTP フォールバックをサポートしている場合に限り録音が許可され、レコーダに対するメディアストリームが RTP にフォールバックされます。

認証済みの電話機を使用したコールを録音するには:

- 電話を許可するには、Cisco callmanager Service パラメータで **認証済みの電話録音** を設定します。この場合、コールは認証されますが、録音サーバへの接続は非認証であり、暗号化されません。
- クラスタ **SIPOAuth Mode** フィールドが Cisco callmanager enterprise パラメータであることを確認します。[有効 (Enabled)] に設定されていることを確認します。

セキュアなコールのモニタリングと録音のセットアップ

セキュアコールのモニタリングと録音を設定するには、次の手順を実行します。

ステップ 1 エージェントおよび上司の電話機でセキュアな機能をプロビジョニングします。

ステップ 2 次の設定を使用して、セキュアな SIP トランクを作成します。

- [デバイスのセキュリティモード (Device Security Mode)] を [暗号化 (Encrypted)] に設定します。
- [セキュリティステータスを送信 (Transmit Security Status)] チェックボックスをオンにします。
- [SRTP を許可する (SRTP Allowed)] チェックボックスをオンにします。
- [TLS SIP トランク (TLS SIP trunk)] をレコーダに設定します。

ステップ 3 非セキュアなモニタリングおよび録音と同じ方法で、モニタリングと録音を設定します。

- a) エージェントの電話の組み込みブリッジを設定します。
- b) エージェントの電話の [ディレクトリ番号 (Directory Number)] ページを使用して、[録音オプション (Recording Option)] ([通話録音の自動有効化 (Automatic Call Recording Enabled)] と [アプリケーションから呼び出されたコール録音が有効 (Application Invoked Call Recording Enabled)]) を設定します。
- c) レコーダのルートパターンを作成します。
- d) ディレクトリ番号にコール録音プロファイルを追加します。
- 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。

詳細な情報と手順については、『[Cisco Unified Communications Manager 機能設定ガイド](#)』の「「モニタリングと録音」」の章を参照してください。



第 25 章

VPN クライアント

- [VPN クライアントの概要 \(321 ページ\)](#)
- [VPN クライアント設定のタスク フロー \(321 ページ\)](#)

VPN クライアントの概要

Cisco Unified IP Phone 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 (322 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 電話 をサポートするための Cisco IOS SSL VPN の設定 (323 ページ) | IP 電話 で VPN クライアントの Cisco IOS を設定します。Cisco IOS VPN を設定するには、このアクションを実行します。 |

| | コマンドまたはアクション | 目的 |
|---------|--|---|
| ステップ 3 | AnyConnect 用の ASA 前提条件への対応 (325 ページ) | AnyConnect 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 電話 での VPN クライアント用の ASA の設定 (325 ページ) | IP 電話で 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 (327 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 (328 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 (329 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 | 次のいずれかの操作を行います。 <ul style="list-style-type: none"> • VPN プロファイルの設定 (330 ページ) • VPN 機能のパラメータの設定 (332 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 Profile] 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 (334 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 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。 | To run the Cisco VPN client, a supported Cisco Unified IP Phone 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細については、ご使用の Cisco Unified IP Phone モデルの Unified Communications Manager に関する <i>Cisco Unified IP</i> 電話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 12 | サポートされている Cisco Unified IP Phone を使用して、VPN 接続を確立します。 | Cisco Unified IP Phone 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。

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 電話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。

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 電話 を認証します。

ステップ 3 から Unified Communications Managercapf 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 ソフトウェア上に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。他の証明書について、この手順を繰り返します。

- d) 次の Cisco IOS 自己署名証明書を作成して 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。

- 自己署名証明書を作成します。

```
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、自己署名証明書を作成します。

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。例：

```
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。

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。
- You can only use a single URL (FQDN or IP address) on the VPN gateway in Unified Communications Manager.
- 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 電話での 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。

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)# route <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。

から次の証明書を Unified Communications Manager 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 電話 の認証。
- CAPF : LSC を使用した IP 電話 の認証。

これら Unified Communications Manager の証明書をインポートするには、次の手順を実行します。

- [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。
- 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。
- 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ついて繰り返します。

- 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。例：

```
ciscoasa(config)# username CP-7975G-SEP001AE2BC16CB password k1kLQGtoxyCO4ti9 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 Phone 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 Phone 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 Phone 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。

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

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 \(327 ページ\)](#)」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。

ステップ 1 [Cisco Unified CM 管理 (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 次のいずれかの操作を行います。

- [**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。
- 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。
- 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 クライアント用 VPN ゲートウェイのフィールド \(329 ページ\)](#)」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 クライアント用 VPN ゲートウェイのフィールド

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 クライアント用 VPN ゲートウェイのフィールド

| 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)] | <p>ゲートウェイのメイン VPN コンセントレータの URL を入力します。</p> <p>(注) グループ URL で VPN コンセントレータを設定し、この URL をゲートウェイの URL として使用する必要があります。</p> <p>設定についての情報は、以下のような VPN コンセントレータのドキュメントを参照してください。</p> <ul style="list-style-type: none"> 『<i>SSL VPN Client (SVC) on ASA with ASDM Configuration Example</i>』 |
| [VPN Certificates in this Gateway] | <p>上矢印キーと下矢印キーを使用して、ゲートウェイに証明書を割り当てます。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。</p> <p>(注) VPN ゲートウェイには最大 10 の証明書を割り当てることができます。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 VPN 信頼ルール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。</p> |

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。

ステップ 1 [Cisco Unified CM 管理 (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 次のいずれかの操作を行います。

- [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。
- 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。
- 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。フィールドの説明の詳細については、「VPN クライアント用 VPN ゲートウェイのフィールド (329 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 クライアント用 VPN グループのフィールド

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 クライアント用 VPN グループのフィールド

| 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 ゲートウェイを確認します。 |
| [この VPN グループ内で選択された VPN ゲートウェイ (Selected VPN Gateways in this VPN Group)] | <p>上矢印キーと下矢印キーを使用して、使用可能な VPN ゲートウェイをこの VPN グループの内外に移動します。</p> <p>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。</p> <p>(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の合計数は10以下にする必要があります。</p> |

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。

ステップ 1 [Cisco Unified CM 管理 (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 次のいずれかの操作を行います。

- 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。フィールドの説明の詳細については、「[VPN クライアント用 VPN プロファイルのフィールド \(331 ページ\)](#)」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 クライアント用 VPN プロファイルのフィールド

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 (Name)] | VPN プロファイルの名前を入力します。 |
| [説明 (Description)] | 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の有効化 (Enable Auto Network Detect)] | このチェックボックスをオンにすると、企業ネットワークの外にいることが検出された場合に限り、VPN クライアントが動作します。 デフォルトで、ディセーブルになっています。 |
| [最大伝送ユニット (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。 デフォルト値: 1290 バイト |
| [接続に失敗 (Fail to Connect)] | このフィールドは、システムが VPN トンネルを作成している間に、ログイン操作または接続操作が完了するのを待機する時間を指定します。 デフォルト: 30 秒 |
| [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をオンにする場合、ゲートウェイ証明書 subjectAltName または CN は、VPN クライアントの接続先の URL と一致する必要があります。 デフォルト: 有効 |

| フィールド | 定義 |
|--|--|
| [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、クライアントの認証方式を選択します。 <ul style="list-style-type: none"> • [ユーザおよびパスワード (User and Password)] • パスワードのみ • [証明書 (LSC または MIC) (Certificate (LSC or MIC))] |
| [パスワードの永続化を有効にする (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

ステップ 1 [Cisco Unified CM 管理 (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 \(332 ページ\)](#)」を参照してください。

ステップ 3 [保存 (Save)]をクリックします。

次の作業を行います。

- 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。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 Phone モデルの *Cisco Unified IP 電話 アドミニストレーションガイド*を参照してください。
- サポートされている Cisco Unified IP Phone 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の有効化 (Enable Auto Network Detect)] | [はい (True)]の場合、企業ネットワークの外にいたことが検出された場合に限り、VPN クライアントが動作します。 デフォルト : False |

| フィールド | デフォルト |
|--|---|
| MTU | このフィールドは、最大伝送ユニットを指定します。 デフォルト値は 1290 バイトです。 最小値は 256 バイトです。 最大値は 1406 バイトです。 |
| [キープアライブ (Keep alive)] | このフィールドは、システムがキープアライブメッセージを送信するレートを指定します。 (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 最大値 : 120 秒 |
| [接続に失敗 (Fail to Connect)] | このフィールドは、システムが VPN トンネルを作成している間に、ログイン操作または接続操作が完了するのを待機する時間を指定します。 デフォルト : 30 秒 最小値 : 0 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、クライアントの認証方式を選択します。 <ul style="list-style-type: none"> • [ユーザおよびパスワード (User and Password)] • パスワードのみ • [証明書 (LSC または MIC) (Certificate (LSC or MIC))] デフォルト : [ユーザおよびパスワード (User and Password)] |
| [パスワードの永続化を有効にする (Enable Password Persistence)] | [はい (True)]の場合、リセットするために[リセット (Reset)]ボタンまたは「**#**」が使用されると、ユーザパスワードは電話機で保存されます。電話機の電源が失われるか、または工場出荷時の設定にリセットすると、パスワードは失われ、電話機でクレデンシャル用の音声ガイダンスが流れます。 デフォルト : False |

| フィールド | デフォルト |
|---|--|
| [ホストIDチェックを有効化 (Enable Host ID Check)] | [はい (True)] の場合、ゲートウェイ証明書 subjectAltName または CN は、VPN クライアントの接続先の URL と一致する必要があります。 デフォルト : [はい (True)] |

共通の電話プロフィールへの VPN の詳細の追加

一般的な電話プロフィールに VPN の詳細を追加するには、次の手順を使用します。

-
- ステップ 1** [Cisco Unified CM 管理 (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)] > [共通の電話プロフィール (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ィールを選択します。
- 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プロフィール (VPN Profile)] を選択します。
- ステップ 4** [保存 (Save)]、[設定の適用 (Apply Config)] の順にクリックします。
- 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の強化

- [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説明します。以下の項目のいくつかは、シスコの標準製品マニュアルが予定通りに更新される前の項目です。

Unified Communications Manager は、VMware vSphere ESXi に基づく仮想化ハードウェアの最上部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 はクローズ系のターンキーパッケージ化された「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、次の特徴があります。

- 攻撃対象領域を縮小します。
- より安定した、より高いパフォーマンスの設定を提供します。
- 設定エラーによる脆弱性を回避します。
- OS/DB のスキルセットが不要で、管理と修正メンテナンスが簡素化されます。

Unified Communications Manager ワークロードレイヤの主なセキュリティ強化は次のとおりです。

- Unified Communications Manager は、汎用/オープンシステムのワークロードではありません。
 - これは汎用の OS 配布を使用しません。
 - 使用されていないモジュールはイメージから除外され、使用されていないサービスは無効化/削除されています。
 - シスコでは、特定のモジュールに対して独自のセキュリティ強化の変更を行います（たとえば、OpenSSL はシスコの Security and Trust Organization によってセキュリティ強化されています）。その結果、CiscoSSL が製品内に組み込まれます。

- ゲストオペレーティングシステム、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に対するネイティブインターフェイスは公開されません。
 - これらは、削除または非表示およびロックダウンされます。
 - アクセスは、シスコが提供するブラウザベースの GUI、CLI、または API のみを介して、これらのインターフェイスを保護するさまざまな方法（SSH を介した CLI、またはセキュア FTP を介したファイルのプルなど）を使用して行われません。
- 製品は、注意深く制御されるスタックで構成され、スタックはアプリケーションの操作、保守、保護、および管理に必要なすべてのソフトウェアを含んでいます。シスコは、シスコが提供し、デジタル署名されたイメージを介してすべてのソフトウェアを指定、インストール、および更新します。
- 上記のすべての情報は、ここに記載している Cisco Secure Product Lifecycle 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。
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は、上記の制御されたシスコインターフェイスの範囲外の非シスコソフトウェアやソフトウェア更新/変更を挿入することをサポートしません。
 - このワークロード内のすべてのソフトウェアは、シスコによって提供され、デジタル署名され、モノリシックイメージ（.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、および更新するには、シスコが提供する .ISO ファイルまたは .COP ファイルを使用することが唯一の方法です。
 - .ISO ファイルは、シスコイメージ内の 1 つ、一部、またはすべてのソフトウェア要素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、最も一般的なユーザロケールおよび電話機のファームウェアを更新するために使用されます。
 - 以下の設定を有効にすることはできません。
 - ウイルス対策クライアント、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。
 - お客様がアップロード可能または外部でアップロード可能なソフトウェア。
 - サードパーティ製アプリケーション
- ワークロード内のゲスト OS に対する「ルートアクセス」は有効化できません。
 - お客様は、シスコが提供する GUI、CLI、または API で認証を使用します。
 - このワークロードに公開されるインターフェイスはすべて安全です（パスワード複雑性ルールの適用、telnet ではなく SSH、設定可能な最小バージョンの TLS 1.2 など）。

- 通常の GUI/CLI/API を介してフィールドで修正できない緊急の問題の場合、お客様はシスコ テクニカル アシスタンス センター (TAC) のエキスパートがルートアクセスを取得できるよう、一時的な「リモートアカウント」を設定できます。お客様は制御を維持し、自動的に期限切れとなるこのアカウントをオンまたはオフにできます。お客様は、TAC が実行しているすべてのアクションをログに残した状態で、TAC の担当者が実行している内容を確認することができます。
- 組み込み侵入防御機能：
 - ホストベースの侵入保護機能を提供する、SELinux 適用モード。
 - SELinux 適用モードは、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、ジョブに必要な「最小権限」に制限する必須アクセス制御を適用します。
 - 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、適切なポートが開き、そのサーバで使用されるサービスの正しいレート制限を含んでいます。
 - IPTable ルールは、次のコマンドを使用して表示できます。
 - **utils firewall ipv4 list**
 - **utils firewall ipv6 list**

上記のセキュリティ強化機能に加えて、Unified Communications Manager ワークロードにより、OS、DB、およびアプリケーション ソフトウェアのセキュリティ監査ロギングが実行されます。セキュリティ監査ログには次の 3 種類があります。

- Linux 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。

また、構成設定では、システム管理者が組織の infosec 要件に準拠するようシステムを設定することもできます。システム管理者が設定可能なセキュリティ設定とユーティリティには、次のものがあります。

- パスワードポリシーの定義。すべてのパスワードと PIN はハッシュまたは暗号化され、クリアテキストとして保存されません。
- アカウントのロックアウト設定とログイン情報ポリシー。
- 警告バナーテキスト。
- シグナリングとメディアに対する TLS/SRTP の有効化。
- 電話機のセキュリティ強化設定。

- 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 モードまたはコモンクライテリアモードの有効化。
- スマートカードまたはバイOMETリック リーダーのサポートを含む SAML シングルサインオンの有効化。
- すべてのネットワーク接続、プロセス、アクティブパッケージを表示します。
 - 「show network status detail all nodns」 開いているポートの詳細を取得します。"netstat -an" Unix コマンドに相当します。
 - 「show process list detail」 すべてのプロセスと各プロセスに関する重要な情報のリストを取得します。「ps -ef」 Unix コマンドに相当します。
 - 「show packages active」 インストール済みおよび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。

設定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。

シスコの UC 製品は、次を含むさまざまな政府認定への準拠について定期的にテストされ、検証されています。

- Department of Defense Information Network Approved Products List (DoDIN APL)
- FIPS 140-2 レベル 1
- FedRAMP
- Common Criteria
- Applicable U.S. Department of Defense Security Technical Implementation Guides (STIGs)

シスコの政府認定の詳細については、次を参照してください。

<https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications.html>。

セキュリティ脆弱性アラートと管理のために、Unified Communications Manager ワークロード全体が Cisco Product Security Incident Response Team (PSIRT) によってサポートされます。Cisco PSIRT は、Cisco 製品およびネットワークに関連するセキュリティ脆弱性情報の収集、調査、およびレポートの公開を管理する専門のグローバルチームです。次の操作を実行する必要があります。

- 導入環境に影響を及ぼす可能性があるセキュリティの問題に関するアラートについては、シスコ セキュリティ アドバイザリおよびアラートのページ (<https://tools.cisco.com/security/center/publicationListing.x>) を参照してください。
- 影響を受ける製品、ワークロード、および永続的な解決策については、Cisco.com の特定の PSIRT のセキュリティアドバイザリを参照してください。

詳細については、https://tools.cisco.com/security/center/resources/security_vulnerability_policy.htmlを参照してください。



第 **V** 部

トラブルシューティング

- [セキュリティトラブルシューティングの概要 \(343 ページ\)](#)



第 27 章

セキュリティトラブルシューティングの概要

- [リモート アクセス \(343 ページ\)](#)
- [Cisco Secure Telnet \(344 ページ\)](#)
- [リモート アカウントの設定 \(346 ページ\)](#)

リモート アクセス

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 ダイア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
- ダイアルイン 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 Secure Telnet は、Cisco Service Engineers (CSE) がトランスペアレントファイアウォールを使用してユーザのサイトにある Unified Communications Manager サーバにアクセスできる機能を提供します。

Cisco Secure Telnet は、シスコ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、ファイアウォールの変更を行わずに Unified Communications Manager サーバをリモートモニタリングおよびメンテナンスできます。



- (注) シスコは、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。

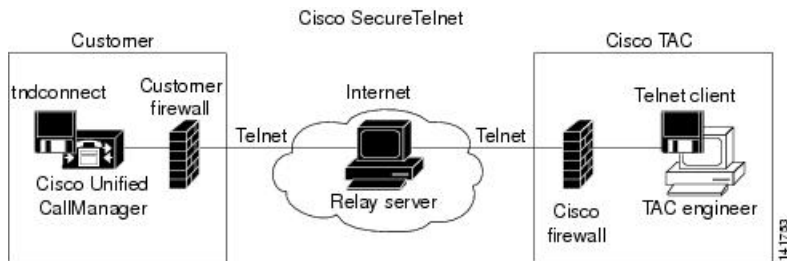
通常、企業ネットワークではパブリックインターネットとの通信が許可されますが、ファイアウォール内部から外部ホストに向けて開始される接続だけが許可されます。

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によって、お客様のネットワークとシスコとの間に 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 アドレスと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。

Telnet 接続が安定した後、CSE はすべてのリモート有用性機能の機能を実装して、Unified Communications Manager サーバ上でメンテナンス、診断、およびトラブルシューティングタスクを実行できます。

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表示することはできますが、コマンドや応答はすべてが完全な形式で表示されるわけではありません。

リモート アカウントの設定

シスコ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に、Unified Communications Manager でリモート アカウントを設定します。

-
- 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、暗号化パスワードを生成します。
 - ステップ 5 シスコの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ワードを提供します。
-

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。