コンフィギュレーション

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。

Table 1: 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	次のようなオプションのセキュリティ機能を設定します。 • セキュアなモニタリングとレコーディング • セキュア会議 • セキュアトーンとアイコン • V.150 • MRA • AS-SIP