目次

概要

この技術情報は Cisco TelePresence System Profile MXP シリーズ、Cisco TelePresence System MXP シリーズ、Cisco Telepresence System Integrator MXP シリーズおよび Cisco TelePresence System Edge MXP シリーズ 製品に関連しています。

Q. コールをですセキュア確認する方法

A. すべての暗号化の方法はよくあるアルゴリズムを使用します。 セキュリティはキーから、それに告げるためにデータを暗号化する方法をアルゴリズムに通じる数来ます。 一般に用いられた通信暗号化の方法はデータ暗号規格（DES）です。 DES は 56 ビット長いキーの暗号化データによってはたらきます。 トリプルDES（トリプル DES）は効果的に 112-bit 長いキーを実行する DES へ機能拡張です。 DES およびトリプル DES はコマーシャルおよび非防御政府通信で今日広く利用されています両方。 DES およびトリプル DES 両方よりセキュリティの高度を提供するために、Advanced Encryption Standard（AES）と呼ばれる新しい規格は開発されました。 128-bit キーの新しい AES 規格は米国政府によって敏感で、分類していないデータを保護するために承認され、ためにトリプル DES の使用を取り替えて下さい。 TANDBERG は次の暗号化 規格すべてをサポートします: H.323、H.320 および専用回線の拡張ディフィー-ヘルマンキー ディストリビューションの AES、DES、H.233、H.234 および H.235。 TANDBERG セキュア会議はデフォルトでオンになっています。 これは自動的に暗号化されたコールを生成します。 画面のロック アイコンを見る場合コールがセキュアであることを確認します。 単一 ロック シンボルは DES のために表示する。 二重ロック シンボルは AES のために表示する。 セキュア会議 DES および AES は ISDN および IP のポイントツーポイント コールおよびマルチポイント呼び出しで利用できます両方完全な TANDBERG 製品ラインの 768 キロビット/秒まで。 TANDBERG の AES および DES 暗号化アルゴリズムの実装は連邦情報処理標準（FIP）に従ってように国立標準技術研究所（NIST）によってみなされているラボによって検証されました。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems