# 目录



# 简介

此条款与思科网真系统配置文件MXP系列、思科网真系统MXP系列，思科网真系统集成商MXP系列和思科网真系统边缘MXP系列产品关连。

## Q. 如何保证呼叫是安全？

A. 所有加密方法使用普通的算法。安全来自密钥，通过对算法告诉它如何加密数据的编号。一个通常被使用的通信加密方法是数据加密标准(DES)。DES工作在加密与56位长密钥的数据旁边。三重DES (3DES)是有效运行112-bit长密钥的增强对DES。DES和3DES在商务和非防御政府通信今天是用途广泛。要提供高度安全比DES和3DES，呼叫高级加密标准(AES)的一个新的标准开发。有128-bit密钥的新的AES标准由美国政府审批保护敏感，未保密的数据，并且请替换使用3DES。TANDBERG支持所有以下加密标准：AES、DES、H.233、H.234和H.235与一延长的迪菲–赫尔曼密钥分配在H.323、H.320和租用的线路。默认情况下TANDBERG安全会议打开。这自动地生成一已加密呼叫。您知道您的呼叫安全，当您看到在您的屏幕的锁定图标。单个锁定符号为DES显示。一个双锁定符号为AES显示。安全会议DES和AES是可用的在点对点呼叫和多点呼叫在ISDN和IP 768 Kbps在全双工TANDBERG产品线。AES和DES加密算法的TANDBERG的实施验证如符合联邦信息处理标准(FIP)由美国标准技术研究所(NIST)检定的实验室。

# 相关信息

- 技术支持和文档 - Cisco Systems