# 安全的敏感数据(SSD)属性的配置在200/300系列被管理的交换机的

## 客观

安全的敏感数据(SSD)保护敏感信息例如密码，允许或者拒绝对敏感数据的用户访问，并且防止配置文件毁损由有恶意的用户。SSD使用passphrases对安全数据。Passphrases类似于在交换机被存储并且使用作为加密密钥的密码。不认识密码短语的设备不能对使用密码短语的unencrypt数据。

本文目标将解释功能可用在*Properties页的SSD*。

## 可适用的设备

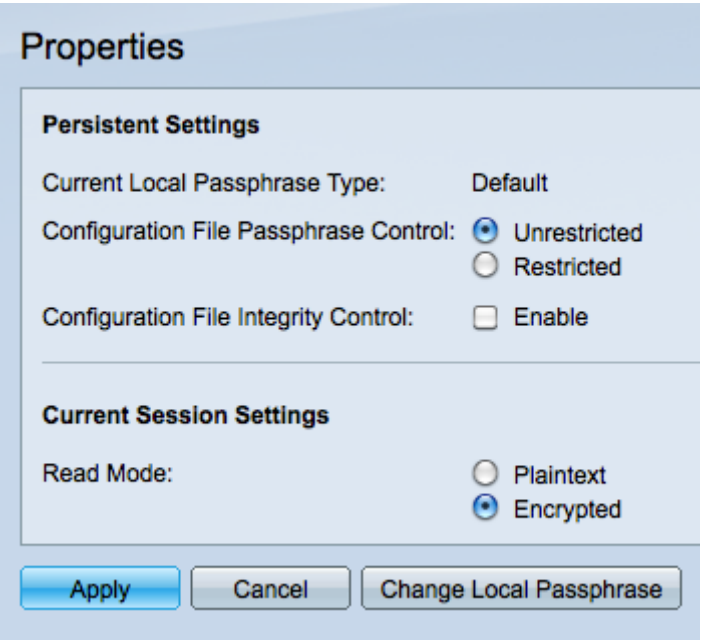
•SF/SG 200和SF/SG 300系列被管理的交换机

## 软件版本

•1.3.0.62

## SSD属性的配置

步骤1.登陆到Web配置工具并且选择**安全>安全的敏感数据Management>属性**。*Properties页*打开：




**Note:**当前本地密码短语控制描述设备是否使用默认密码短语或一用户定义的密码短语。

步骤2.点击在*配置文件密码短语*控制字段的期望单选按钮。

•无限制—发送密码短语到配置文件，允许其它设备认识密码短语。

•有限—从被发送限制密码短语到配置文件，保持从了解密码短语的其它设备。

第 3 步：检查配置文件完整性控制复选框对enable (event)保护免受对配置文件的不需要的修改。

步骤4.在*读的Mode字段*点击期望单选按钮设置文件如何读。

- •明文—使用明文显示当前会话信息。
- •加密—，在显示会话信息前，加密文件。

步骤5.点击**适用**保持当前更改或**取消**取消在页内做的变动。

# 更改本地密码短语

步骤1.登陆到Web配置工具并且选择**安全>安全的敏感数据Management>属性**。点击**更改本地密码短语**。*更改本地密码短语*页打开：

**Note:**当前本地密码短语类型描述哪密码短语是在使用中的。

步骤2.点击从*本地密码短语*字段的期望单选按钮。

- •默认值—使用默认密码短语。
- •用户定义—用户定义了使用什么密码短语。

第 3 步：如果用户定义在*确认密码字段*点击，进入期望密码短语字段，然后送进同样密码短语。

步骤4.选择**适用**保持变动做或**取消**取消在此页的所有更改。

步骤5.选择**回到**回归到*Properties页*。