200/300系列管理型交换机上的安全敏感数据(SSD)属性配置

目标

安全敏感数据(SSD)可保护密码等敏感信息，允许或拒绝用户访问敏感数据，并防止配置文件被恶意用户损坏。SSD使用密码保护数据。密码短语类似于存储在交换机中并用作加密密钥的密码。不知道该口令的设备将无法对使用该口令的数据进行解密。

本文档旨在说明SSD Properties页面中可用的功能。

适用设备

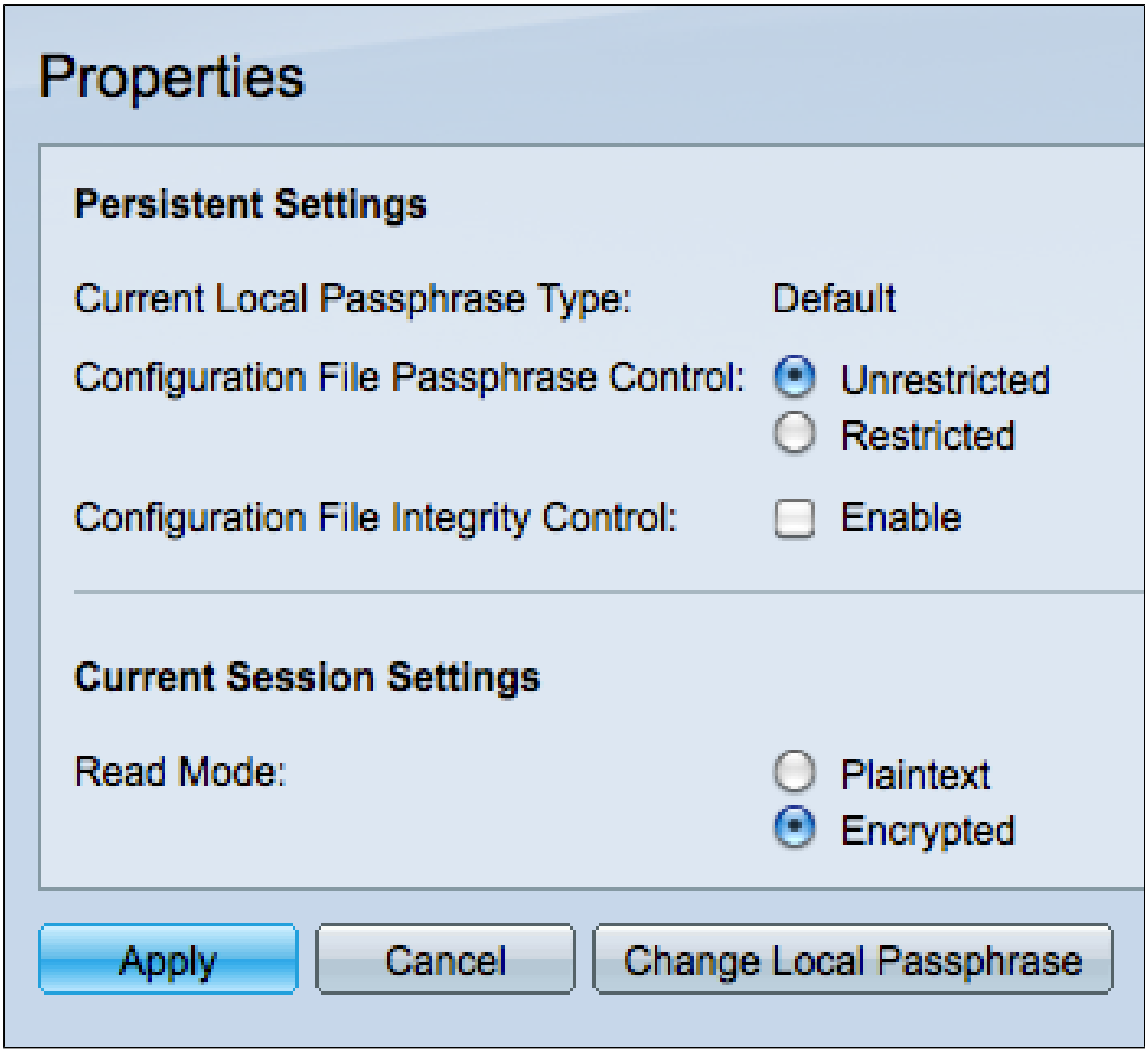
· SF/SG 200和SF/SG 300系列托管交换机

软件版本

•1.3.0.62

SSD属性的配置

步骤1:登录到Web配置实用程序，然后选择Security > Secure Sensitive Data Management > Properties。将打开Properties页面：



注意：Current Local Passphrase Control说明设备是使用默认密码还是使用用户定义的密码。

第二步：点击Configuration File Passphrase Control字段中所需的单选按钮。

·不受限制 — 将密码发送到配置文件，使其他设备可以知道该密码。

·受限 — 限制将密码发送到配置文件，以防止其他设备获知该密码。

第三步：选中Configuration File Integrity Control复选框以启用保护，防止对配置文件进行不需要的修改。

第四步：单击Read Mode字段中的所需单选按钮以设置文件的读取方式。

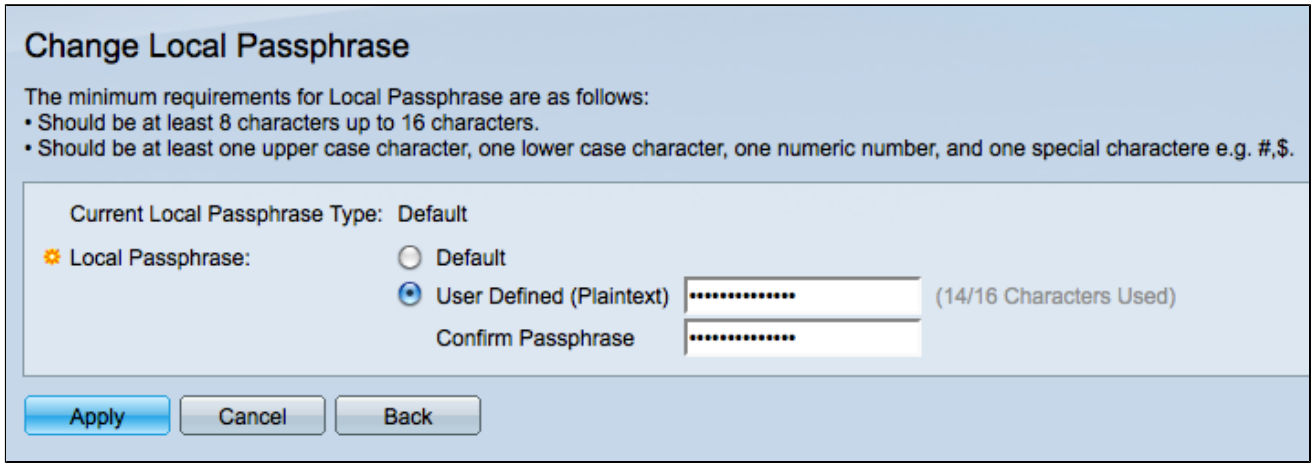
·纯文本 — 使用纯文本显示当前会话信息。

·已加密 — 在文件显示会话信息之前对其进行加密。

第五步：单击Apply以保留当前更改，或单击Cancel以撤消在页面中进行的更改。

更改本地密码

步骤1:登录到Web配置实用程序，然后选择Security > Secure Sensitive Data Management > Properties。单击更改本地密码。Change Local Passphrase页打开：



注意：当前本地密码类型描述了正在使用的密码。

第二步：从Local Passphrase（本地密码）字段点击所需的单选按钮。

·默认 — 使用默认密码。

·用户定义 — 用户定义使用的密码。

第三步：如果点击User Defined，请在字段中输入所需的密码，然后在Confirm Password字段中输入相同的密码。

第四步：选择Apply以保留所做的更改，或选择Cancel以撤消此页上的所有更改。

第五步：选择Back以返回到Properties页。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。