安全的敏感数据(SSD)规则的创建和管理在200/300系列被管理的交换机的

客观

此条款显示您如何设置和管理安全的敏感数据的(SSD)规则在200/300系列交换机。

可适用的设备

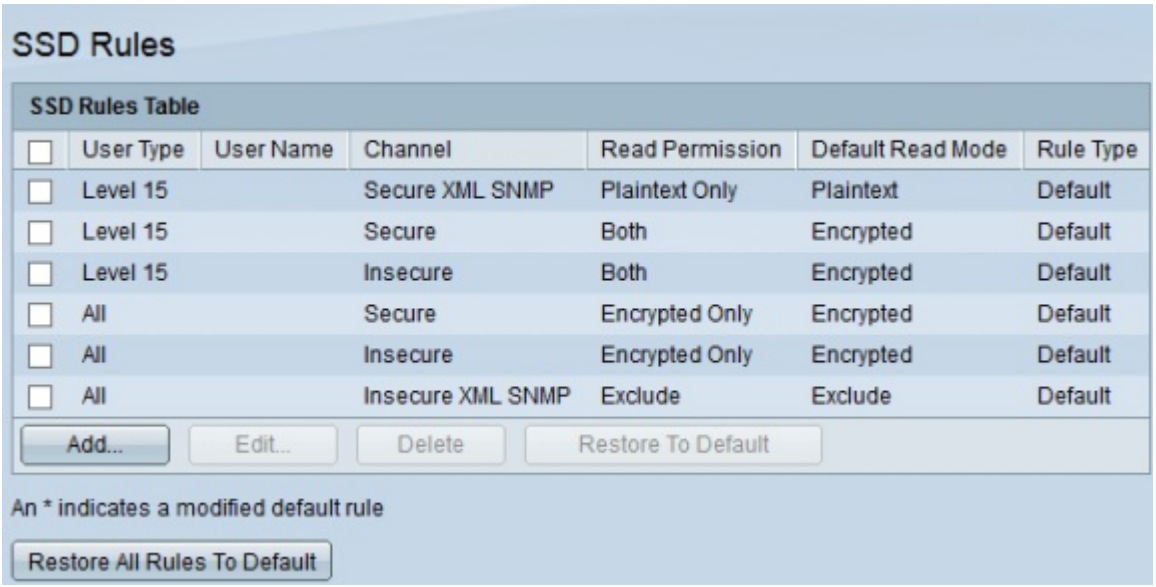
•SF/SG 200和SF/SG 300系列被管理的交换机

软件版本

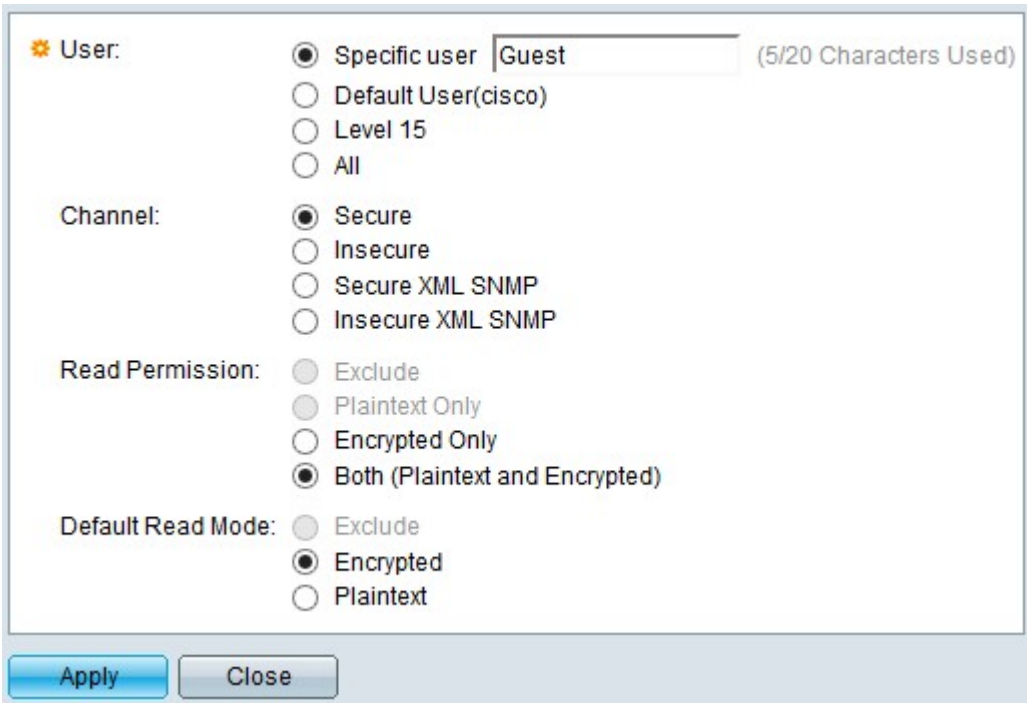
•v1.2.7.76

SSD规则

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> SSD规则**。*SSD规则*页出版。



Step 2.要创建新规则，请点击**添加**。*规则定义*页打开。



第 3 步：在用户字段，请选择运用规则的用户的一个单选按钮选择。

•特定用户—，如果规则适用于单个用户，请输入特定用户名字段。

•默认用户—。此规则适用于默认用户，设置为cisco。

•第15级—此规则适用于所有用户有第15级权限。

•全此规则适用于所有用户。

第 4 步：在*信道*领域，请选择一个单选按钮确定适用于规则的哪些信道。

•巩固—只做此规则适用于安全信道。这包括控制台，不是SSH和HTTPS，但是XML信道。

•不安全—只做此规则适用于不安全的信道。这包括不是Telnet、TFTP和HTTP，但是XML信道。

•获取XML SNMP —只做此规则适用于在HTTPS的XML与保密性。

•不安全的XML SNMP —只做此规则适用于XML在HTTP或没有保密性。

第 5 步：在*读的权限*字段，请根据您的早先选择选择一个单选按钮。

•如果，在第3步，选择了第15级或全部，请点击**排除**或**仅明文。**

•如果，在第4步，选择了安全的XML SNMP或不安全的XML SNMP，请点击**排除**或**仅明文。**

•如果，在第4步，选择了安全或不安全请点击**只加密**或**两个(明文和加密)。**

第6.步。在*读的默认值Mode字段*，点击**排除**，**加密**或者**明文。**

第 7 步：要启动规则，请点击**适用**。要取消规则创建，请点击**Close。**


SSD Rules
SSD Rules Table
User Type
User Name
Channel
Read Permission
Default Read Mode
Rule Type
Specific
Guest
Secure
Both
Encrypted
User Defined
Level 15
Secure XML SNMP
Plaintext Only
Plaintext
Default
Level 15
Secure
Both
Encrypted
Default
Level 15
Insecure
Both
Encrypted
Default
All
Secure
Encrypted Only
Encrypted
Default
All
Insecure
Encrypted Only
Encrypted
Default
All
Insecure XML SNMP
Exclude
Exclude
Default
Add...
Edit...
Delete
Restore To Default
An * indicates a modified default rule
Restore All Rules To Default