

# 802.1x认证的配置在SFE/SGE的管理了交换机

## 目标

此条款说明关于802.1x在SFE/SGE被管理的交换机的端口认证的配置。802.1x是基于端口的网络访问控制一个IEEE标准。认证用于配置在每个端口的802.1x安全参数。证明人操作类似治安警卫对一个受保护的网路。802.1x允许请求方请求从被连接的证明人设备的端口访问。请求方能发送数据到端口，如果请求方验证并且被核准，或者丢弃它。

## 可适用的设备

- SFE/SGE被管理的交换机

## 软件版本

- v3.0.2.0

## 端口认证

步骤1. 登录到Web配置工具选择安全套件> 802.1X >认证。认证页打开：

| Authentication |                     |                     |       |                |                   |                      |      |
|----------------|---------------------|---------------------|-------|----------------|-------------------|----------------------|------|
| Port           | Host Authentication | Action on Violation | Traps | Trap Frequency | Status            | Number of Violations |      |
| 1/e1           | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |
| 1/e2           | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |
| 1/e3           | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |
| 1/e4           | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |
| 1/e5           | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |
| 1/e6           | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |
| 1/e7           | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |
| 1/e8           | Multiple Host       |                     |       |                | Not in auto mode  | 0                    | Edit |
| 1/e9           | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |
| 1/e10          | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |
| 1/e11          | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |
| 1/e12          | Multiple Host       |                     |       |                | Not in auto mode* | 0                    | Edit |

步骤2. 点击编辑。编辑主机认证窗口出现：

## Edit Host Authentication

|                     |                                     |
|---------------------|-------------------------------------|
| Port                | 1/e1 ▾                              |
| Host Authentication | Single ▾                            |
| Action on Violation | Discard ▾                           |
| Enable Traps        | <input checked="" type="checkbox"/> |
| Trap Frequency      | 10                                  |

**Apply**

从配置的端口下拉列表的步骤3.Choose端口。

## Edit Host Authentication

|                            |  |
|----------------------------|--|
| Port                       | 1/e1 ▾   |
| <b>Host Authentication</b> | Single ▾<br>Single<br>Multiple Host<br>Multi Session |
| Action on Violation        |  |
| Enable Traps               |  |
| Trap Frequency             | 10   |

**Apply**

步骤4.从主机认证下拉列表选择主机认证。

- 单一的被核准的端口可以由客户端获取。
- 多台主机—对于单个可用的端口，广泛客户端可以连接。一旦其中一个客户端被核准访问网络，所有客户端访问。否则访问为所有客户端被拒绝。
- 提供多会话特定的被核准的主机对网络的访问。

## Edit Host Authentication

|                            |  |
|----------------------------|--|
| Port                       | 1/e1 ▾                                       |
| Host Authentication        | Single ▾                                     |
| <b>Action on Violation</b> | Discard ▾<br>Discard<br>Forward<br>Shut Down |
| Enable Traps               |  |
| Trap Frequency             |  |

**Apply**

步骤5.从对侵害下拉列表的动作选择选项。它定义了应采取的措施对的信息包 单个主机模式，在端口被核准后，任何MAC地址接收除客户端的原因侵害之外。

- 丢弃—它丢弃根据用户地址的信息包。

- 前言—，如果用户地址是列出的，它转发信息包。
- 关闭—端口被关闭，直到重置设备。

### Edit Host Authentication

|                     |                                     |
|---------------------|-------------------------------------|
| Port                | 1/e1                                |
| Host Authentication | Single                              |
| Action on Violation | Discard                             |
| Enable Traps        | <input checked="" type="checkbox"/> |
| Trap Frequency      | 10                                  |

Apply

第6步。检查Enable (event)陷阱对在设备的enable (event)陷阱。只有当从在第4步，选择单个这是可用的。

### Edit Host Authentication

|                     |                                     |
|---------------------|-------------------------------------|
| Port                | 1/e1                                |
| Host Authentication | Single                              |
| Action on Violation | Discard                             |
| Enable Traps        | <input checked="" type="checkbox"/> |
| Trap Frequency      | 10                                  |

Apply

步骤7.输入值在陷阱频率区域。范围是从1到1000000，并且DEFAULT值是10。

步骤8.点击**适用**。

**警告：**这只保存您的配置对运行配置文件。这意味着做的所有变动将丢失，如果重新启动设备。如果希望在系统重新启动以后保存这些更改，您需要复制运行配置文件到启动配置文件。请参阅复制在SFE/SGE系列被管理的交换机的配置文件关于如何执行此的更多信息。