# 通过CLI配置在交换机的全局802.1x属性

## Introduction

IEEE 802.1x是实现在客户端和服务器之间的访问控制的标准。在服务可以为客户端提供由一个局部访问网(LAN)前或交换机，客户端被联络到交换端口必须由运行远程验证拨入用户服务(RADIUS)的认证服务器验证。

802.1x认证从连接限制未授权的客户端到LAN通过公共可访问的端口。802.1x认证是客户服务器模型。在此型号，网络设备有以下特定角色：

- 客户端或请求方—客户端或请求方是请求对LAN的访问的网络设备。客户端被联络到证明人。
- 证明人—证明人是提供网络服务的网络设备，并且对哪些请求方端口被连接。支持以下认证方法：

  -基于802.1X —支持在所有认证模式下。使用RADIUS协议，在基于802.1X的认证，证明人从802.1x消息或EAP over LAN (EAPOL)信息包提取可扩展的认证协议(EAP)消息，并且通过他们到认证服务器。

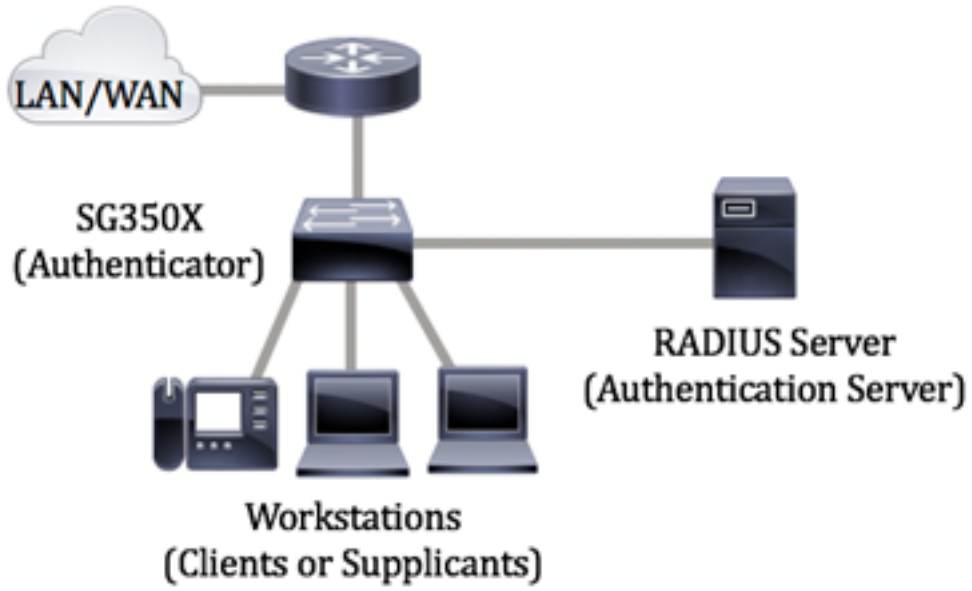
  -基于MAC的—支持在所有认证模式下。当媒体访问控制(MAC) -根据，证明人代表寻找网络访问的客户端执行软件的EAP客户机零件。

  -基于Web的—仅支持在多会话模式下。使用基于Web的认证，证明人代表寻找网络访问的客户端执行软件的EAP客户机零件。

- 认证服务器—认证服务器进行客户端的实际认证。设备的认证服务器是有EAP扩展的一个RADIUS验证服务器。

**Note:**网络设备可以是客户端或请求方，证明人或者两个每个端口。

下面的镜像显示根据特定角色配置了设备的网络。在本例中，使用SG350X交换机。




**在配置802.1x的指南：**

1. 配置RADIUS服务器。要了解如何配置在您的交换机的RADIUS服务器设置，请点击此处。

2. 配置虚拟局域网(VLAN)。使用您的交换机的基于Web的工具，要创建VLAN，请点击此处。对于基于CLI的指令，请点击此处。
3. 配置端口对在您的交换机的VLAN设置。使用基于Web的工具，要配置，请点击此处。要使用CLI，请点击此处。
4. 配置在交换机的全局802.1x属性。关于关于如何的说明通过交换机的基于Web的工具配置全局802.1x属性，请点击此处。
5. (可选)请配置在交换机的时间范围。要了解如何配置在您的交换机的时间范围设置，请点击此处。
6. 配置802.1x端口认证。要使用交换机的基于Web的工具，请点击此处。要使用CLI，请点击此处。

# 客观

此条款提供指令关于怎样通过交换机的命令行界面(CLI)配置全局802.1x属性，包括认证和客户VLAN属性。客户VLAN提供存取对于不需要通过802.1x，基于MAC的或者基于Web的认证或端口将验证和被核准的预订的设备的服务。

# 可适用的设备

- Sx300系列
- Sx350系列
- SG350X系列
- Sx500系列
- Sx550X系列

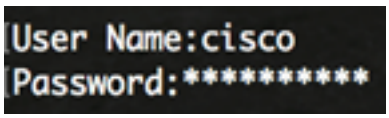
# 软件版本

- 1.4.7.06 — Sx300， Sx500
- 2.2.8.04 — Sx350， SG350X， Sx550X

# 通过CLI配置在交换机的802.1x属性

## 配置802.1x设置

步骤1.交换机控制台的洛金。默认用户名和密码是cisco/cisco。如果配置了一个新的用户名或密码，请输入证件。



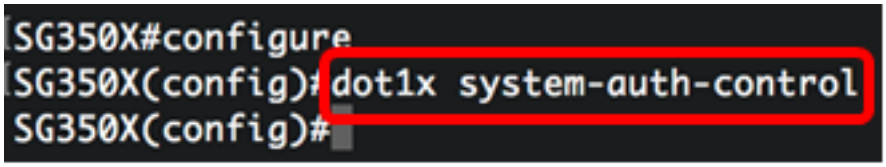

**Note:**命令可能根据您的交换机确切的模型变化。在本例中， SG350X交换机通过Telnet被获取。

**Step 2.**从交换机的Privileged EXEC模式，请通过输入以下输入全局配置模式：

```
SG350x#configure
```

第 3 步：对全局enable (event)在交换机的802.1x认证，请使用**dot1x系统auth控制**in命令全局配置模式。

```
SG350x(config)#dotx1auth
```




第4.步(可选)全局禁用在交换机的802.1x认证，输入以下：

```
SG350x(config)#no dotx1auth
```

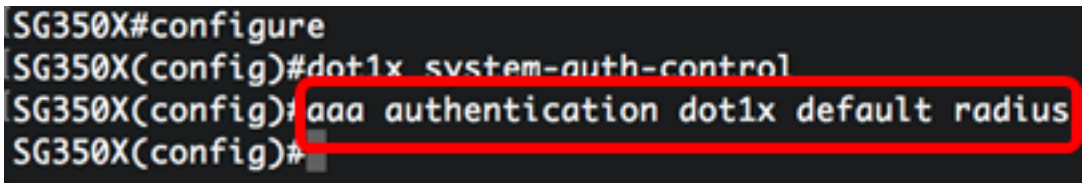
**Note:**如果这是失效的， 802.1X，基于MAC的和基于Web的认证是失效的。

第 5 步：要指定哪些服务器使用认证，当802.1x认证是启用的时，请输入以下：

```
SG350x(config)#aaadot1x[|||]
```

选项是：

- 半径无—这在RADIUS服务器帮助下首先进行端口认证。如果没有自服务器的无响应例如，当服务器发生故障时，则认证没有进行，并且会话允许。如果服务器是可用的，并且用户凭证是不正确的，则访问被拒绝，并且结束会话。
- 半径—这进行根据RADIUS服务器的端口认证。如果没有进行的认证，则会话被终止。这是默认验证。
- 什么都—不验证用户并且允许会话。




**Note:**在本例中，默认802.1x认证服务器是RADIUS。

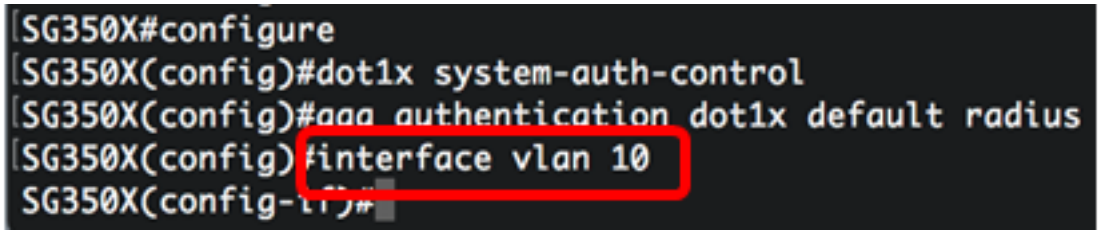
第6.步(可选)恢复默认验证，输入以下：

```
SG350X(config)#no aaa authetication dot1x
```

第 7 步：在全局配置模式下，请通过输入以下进入VLAN接口配置上下文：

```
SG350X(config)#interface VLAN [vlan-id]
```

- vlan-id —指定将被配置的VLAN ID。




第8.步。对enable (event)使用未授权的端口的一个客户VLAN，输入以下：

```
SG350X(config-if)#dot1xVLAN
```

**Note:**如果客户VLAN是启用的，所有未授权的端口自动地加入在客户选择的VLAN VLAN。如

果端口以后被核准，从客户VLAN被去除。

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#interface vlan 10
SG350X(config-if)#dot1x guest-vlan
SG350X(config-if)#
```

第9.步。要退出接口配置上下文，请输入以下：

```
SG350X(config-if)#exit
```

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#interface vlan 10
SG350X(config-if)#dot1x guest-vlan
SG350X(config-if)#exit
SG350X(config)#
```

第10.步。要设置时间延迟在启用802.1X (或端口)和添加端口之间到客户VLAN，请输入以下：

```
SG350X(config)#dot1xVLAN[timeout]
```

- 超时—以在启用802.1X (或端口)和添加端口之间的秒钟指定时间延迟到客户VLAN。范围是从30 180秒。

**Note:**在联结以后，如果软件不发现一802.1x请求方或，如果端口认证发生了故障，然后端口被添加到客户VLAN，在客户VLAN超时周期到期之后。如果端口从核准更改到没核准，端口被添加到客户VLAN，在客户VLAN超时周期到期之后。您能从VLAN认证的enable (event)或功能失效VLAN认证。

```
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#
```

**Note:**在本例中，使用的客户VLAN超时是60秒。

第11.步。对enable (event)陷井，请检查一个或很多以下选项：

```
SG350X(config)# dot1x[||] [802.1x|mac|Web]
```

选项是：

- 802.1x认证失败陷井—，如果802.1x认证发生故障，请发送陷井。
- 802.1x认证成功陷井—，如果802.1x认证成功，请发送陷井。
- MAC验证故障陷井—，如果MAC验证发生故障，请发送陷井。
- mac认证成功陷井—，如果MAC验证成功，请发送陷井。
- Web认证失败陷井—，如果Web认证发生故障，请发送陷井。
- Web认证成功陷井—，如果Web认证成功，请发送陷井。

- Web认证沉寂陷井—，如果一个安静周期开始，请发送陷井。

**Note:**在本例中， 802.1x认证失败和成功陷井被输入。

```
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#dot1x traps authentication success 802.1x
SG350X(config)#dot1x traps authentication failure 802.1x
SG350X(config)#
```

步骤12。要退出接口配置上下文，请输入以下：

```
SG350X(config)#exit
```

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#interface vlan 10
SG350X(config-if)#dot1x guest-vlan
SG350X(config-if)#exit
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#dot1x traps authentication success 802.1x
SG350X(config)#dot1x traps authentication failure 802.1x
SG350X(config)#exit
SG350X#
```

第13步。(可选)显示在交换机的被配置的全局802.1x属性，请输入以下：

```
SG350X#show dot1x
```

```
SG350X(config)#exit
SG350X#show dot1x

Authentication is enabled
Authenticating Servers: Radius
Unauthenticated VLANs: 20
Guest VLAN: VLAN 10, timeout 60 sec
Authentication failure traps are enabled for 802.1x
Authentication success traps are enabled for 802.1x
Authentication quiet traps are disabled
```

您应该成功当前配置了在您的交换机的802.1x属性。

## 配置VLAN认证

当802.1x是启用的时，未授权的端口或设备没有允许访问VLAN，除非他们是客户VLAN的部分或未经鉴定的VLAN。将手工被添加的端口到VLAN。

要禁用在VLAN的认证，请遵从这些步骤：

第 1 步：从交换机的Privileged EXEC模式，请通过输入以下输入全局配置模式：

```
SG350X#configure
```

**Step 2.**在全局配置模式下，请通过输入以下进入VLAN接口配置上下文：

```
KSG350x(config)#VLAN [vlan-id]
```

- vlan-id —指定将被配置的VLAN ID。

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#
```

**Note:**在本例中， VLAN 20被选择。

第 3 步：要禁用在VLAN的802.1x认证，请输入以下：

SG350X(config-if)#dot1x authreq

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#dot1x auth-not-req
SG350X(config-if)#
```

对enable (event) 802.1x认证的第4.步(可选)在VLAN，输入以下：

SG350X(config-if)#no dot1x authreq

第 5 步：要退出接口配置上下文，请输入以下：

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#dot1x auth-not-req
SG350X(config-if)#end
SG350X#
```

第6.步(可选)显示在交换机的802.1x全局认证设置，输入以下：

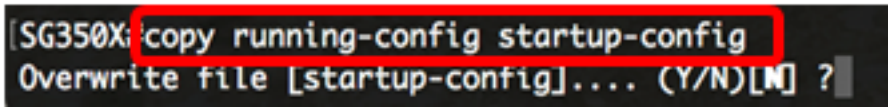
```
SG350X(config-if)#end
SG350X#show dot1x

Authentication is enabled
Authenticating Servers: Radius
Unauthenticated VLANs: 20
Guest VLAN: VLAN 10, timeout 60 sec
Authentication failure traps are enabled for 802.1x
Authentication success traps are enabled for 802.1x
Authentication quiet traps are disabled
```

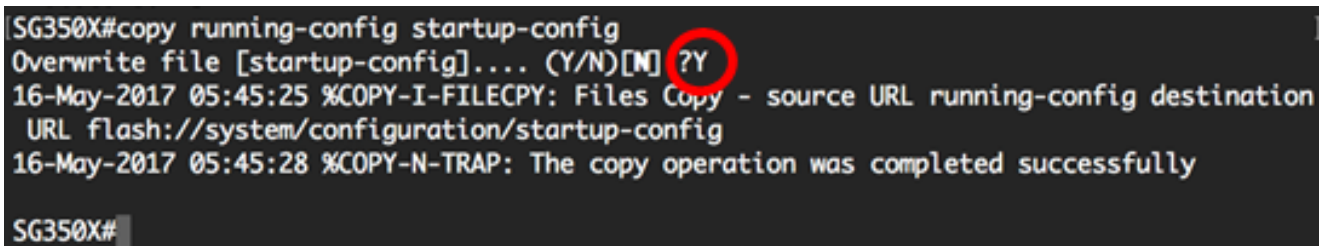
**Note:**在本例中， VLAN 20显示作为未经鉴定的VLAN。

第7.步(可选)在交换机的Privileged EXEC模式下，保存被配置的设置对启动配置文件，通过输入以下：

```
SG350X#copy running-config startup-config
```




第8.步(可选)按是的**Y**或**N**为不在您的关键董事会，一旦重写文件[startup-config]…提示出现。




您应该成功当前配置了在VLAN的802.1x认证设置在您的交换机。

**重要信息**：要继续进行配置在您的交换机的802.1x端口认证设置，请遵从上面指南。