Configure Global 802.1x Properties on a Switch through the CLI

Introduction

IEEE 802.1x is a standard which facilitates access control between a client and a server. Before services can be provided to a client by a Local Access Network (LAN) or switch, the client connected to the switch port has to be authenticated by the authentication server which runs Remote Authentication Dial-In User Service (RADIUS).

802.1x authentication restricts unauthorized clients from connecting to a LAN through publicly-accessible ports. 802.1x authentication is a client-server model. In this model, network devices have the following specific roles:

- Client or supplicant — A client or supplicant is a network device that requests access to the LAN. The client is connected to an authenticator.
- Authenticator — An authenticator is a network device that provides network services and to which supplicant ports are connected. The following authentication methods are supported:

  - 802.1x-based — Supported in all authentication modes. In 802.1x-based authentication, the authenticator extracts the Extensible Authentication Protocol (EAP) messages from the 802.1x messages or EAP over LAN (EAPoL) packets, and passes them to the authentication server, using the RADIUS protocol.

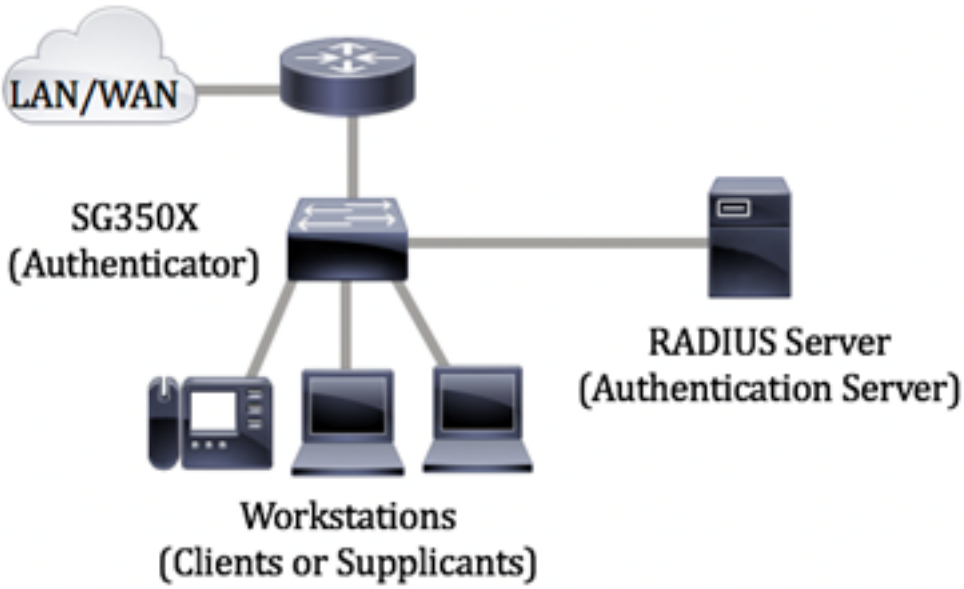
  - MAC-based — Supported in all authentication modes. With Media Access Control (MAC)-based, the authenticator itself executes the EAP client part of the software on behalf of the clients seeking network access.

  - Web-based — Supported only in multi-sessions modes. With web-based authentication, the authenticator itself executes the EAP client part of the software on behalf of the clients seeking network access.

- Authentication server — An authentication server performs the actual authentication of the client. The authentication server for the device is a RADIUS authentication server with EAP extensions.

Note: A network device can be either a client or supplicant, authenticator, or both per port.

The image below displays a network that have configured the devices according to the specific roles. In this example, an SG350X switch is used.



Guidelines in configuring 802.1x:

1. Configure the RADIUS server. To learn how to configure the RADIUS server settings on your switch, click here.
2. Configure Virtual Local Area Networks (VLANs). To create VLANs using the web-based utility of your switch, click here. For CLI-based instructions, click here.
3. Configure Port to VLAN settings on your switch. To configure using the web-based utility, click here. To use the CLI, click here.
4. Configure the global 802.1x properties on the switch. For instructions on how to configure the global 802.1x properties through the web-based utility of the switch, click here.
5. (Optional) Configure Time Range on the switch. To learn how to configure time range settings on your switch, click here.
6. Configure 802.1x Port Authentication. To use the web-based utility of the switch, click here.

Objective

This article provides instructions on how to configure global 802.1x properties through the Command Line Interface (CLI) of the switch, which include authentication and guest VLAN properties. Guest VLAN provides access to services that do not require the subscribing devices or ports to be authenticated and authorized via 802.1x, MAC-based, or web-based authentication.

Applicable Devices

- Sx300 Series
- Sx350 Series
- SG350X Series
- Sx500 Series
- Sx550X Series

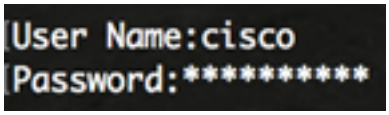
Software Version

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

Configure 802.1x Properties on a Switch through the CLI

Configure 802.1x Settings

Step 1. Log in to the switch console. The default username and password is cisco/cisco. If you have configured a new username or password, enter the credentials instead.



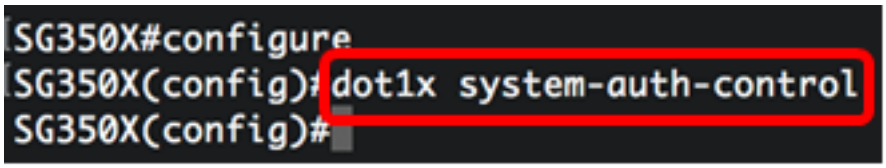
Note: The commands may vary depending on the exact model of your switch. In this example, the SG350X switch is accessed through Telnet.

Step 2. From the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:

```
SG350X#configure
```

Step 3. To globally enable 802.1x authentication on the switch, use the **dot1x system-auth-control** command in Global Configuration mode.

```
SG350x(config)#dotx1 system-auth-control
```



Step 4. (Optional) To globally disable 802.1x authentication on the switch, enter the following:

```
SG350x(config)#no dotx1 system-auth-control
```

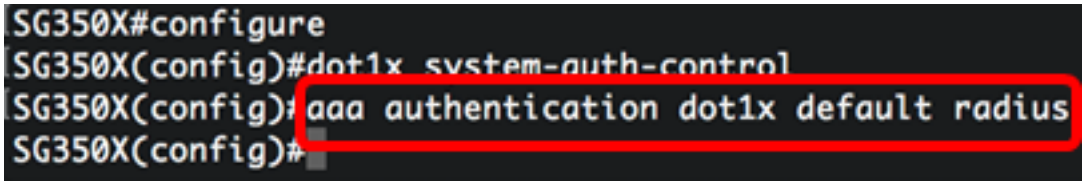
Note: If this is disabled, 802.1X, MAC-based and web-based authentications are disabled.

Step 5. To specify which servers are used for authentication when 802.1x authentication is enabled, enter the following:

```
SG350x(config)#aaa authentication dot1x default [radius none | radius | none]
```

The options are:

- radius none — This performs the port authentication first with the help of the RADIUS Server. If there is no response from the server such as when the server is down, then no authentication is performed and the session is permitted. If the server is available and the user credentials are incorrect, then access is denied and the session is ended.
- radius — This performs the port authentication based on the RADIUS Server. If there is no authentication performed, then the session is terminated. This is the default authentication.
- none — Does not authenticate the user and permits the session.



Note: In this example, the default 802.1x authentication server is RADIUS.

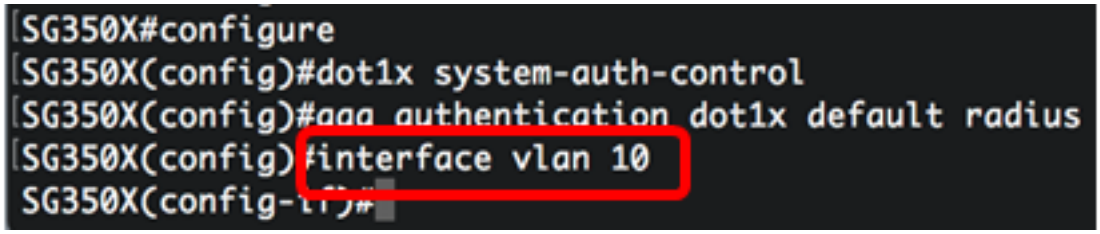
Step 6. (Optional) To restore the default authentication, enter the following:

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

Step 7. In the Global Configuration mode, enter the VLAN Interface Configuration context by entering the following:

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

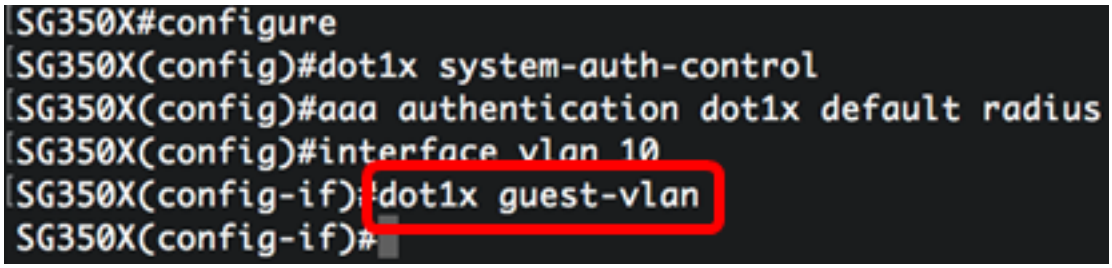
- vlan-id — Specifies a VLAN ID to be configured.



Step 8. To enable the use of a guest VLAN for unauthorized ports, enter the following:

```
SG350X(config-if)#dot1x guest-vlan
```

Note: If a Guest VLAN is enabled, all unauthorized ports automatically join the VLAN chosen in the Guest VLAN. If a port is later authorized, it is removed from the Guest VLAN.



Step 9. To exit the Interface Configuration context, enter the following:

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

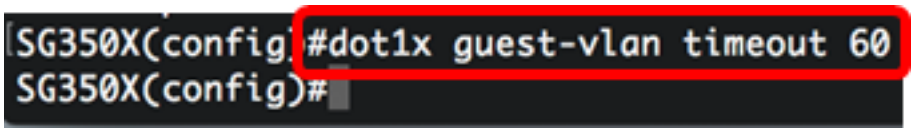


Step 10. To set the time delay between enabling 802.1X (or port up) and adding a port to the guest VLAN, enter the following:

```
SG350X(config)#dot1x guest-vlan timeout [timeout]
```

- timeout — Specifies the time delay in seconds between enabling 802.1X (or port up) and adding the port to the guest VLAN. The range is from 30 up to 180 seconds.

Note: After linkup, if the software does not detect an 802.1x supplicant or if the port authentication has failed, then the port is added to the guest VLAN only after the Guest VLAN Timeout period expires. If the port changes from Authorized to Not Authorized, the port is added to the Guest VLAN only after the Guest VLAN Timeout period expires. You can enable or disable VLAN authentication from the VLAN Authentication.



Note: In this example, the Guest VLAN Timeout used is 60 seconds.

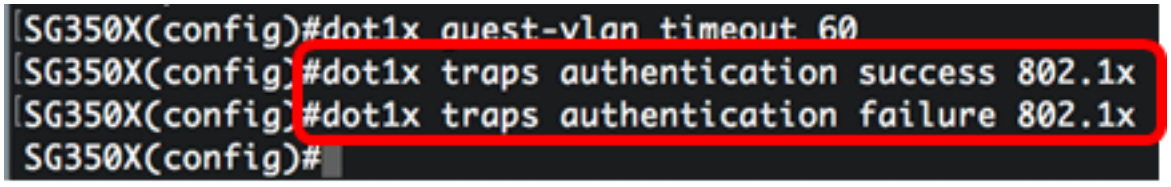
Step 11. To enable traps, check one or more of the following options:

```
SG350X(config)# dot1x traps authentication [failure | success | quiet] [802.1x | mac | web]
```

The options are:

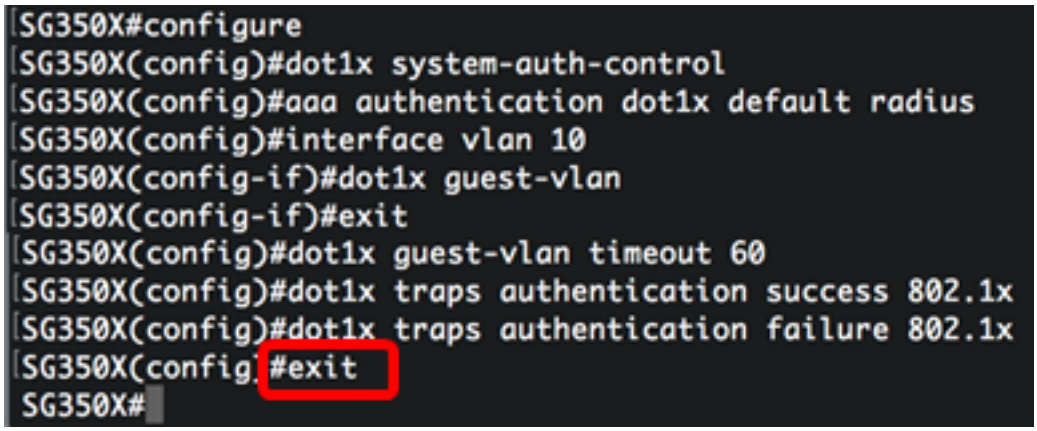
- 802.1x authentication failure traps — Send traps if 802.1x authentication fails.
- 802.1x authentication success traps — Send traps if 802.1x authentication succeeds.
- mac authentication failure traps — Send traps if MAC authentication fails.
- mac authentication success traps — Send traps if MAC authentication succeeds.
- web authentication failure traps — Send traps if Web authentication fails.
- web authentication success traps — Send traps if Web authentication succeeds.
- web authentication quiet traps — Send traps if a quiet period commences.

Note: In this example, 802.1x authentication failure and success traps are entered.



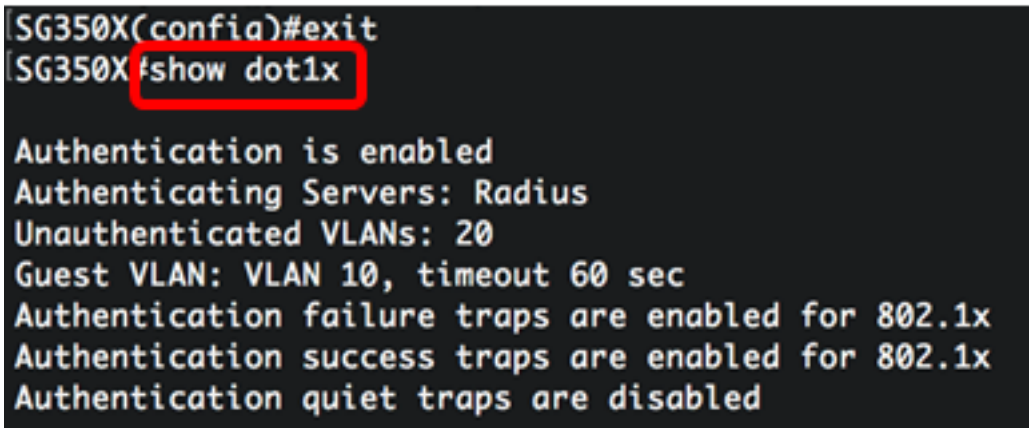
Step 12. To exit the Interface Configuration context, enter the following:

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



Step 13. (Optional) To display the configured global 802.1x properties on the switch, enter the following:

```
SG350X#show dot1x
```



You should now have successfully configured the 802.1x properties on your switch.

Configure VLAN Authentication

When 802.1x is enabled, unauthorized ports or devices are not allowed to access the VLAN unless they are a part of the Guest VLAN or an Unauthenticated VLAN. The ports need to be added manually to VLANs.

To disable authentication on a VLAN, follow these steps:

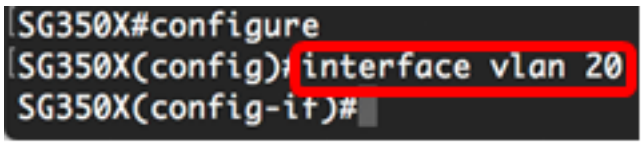
Step 1. From the Privileged EXEC mode of the switch, enter the Global Configuration mode by entering the following:

```
SG350X#configure
```

Step 2. In the Global Configuration mode, enter the VLAN Interface Configuration context by entering the following:

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

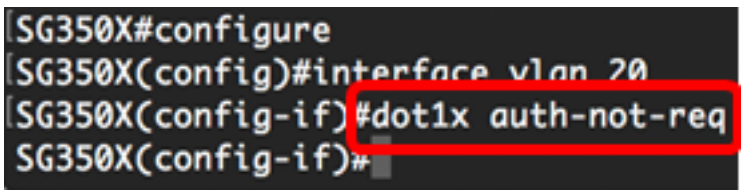
- vlan-id — Specifies a VLAN ID to be configured.



Note: In this example, VLAN 20 is chosen.

Step 3. To disable 802.1x authentication on the VLAN, enter the following:

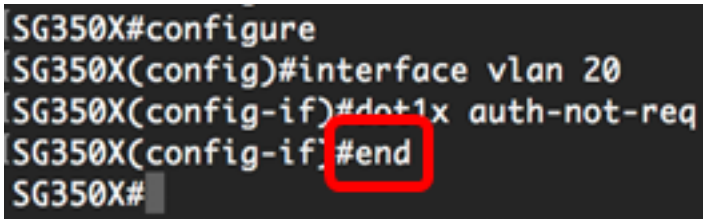
SG350X(config-if)#dot1x auth-not-req



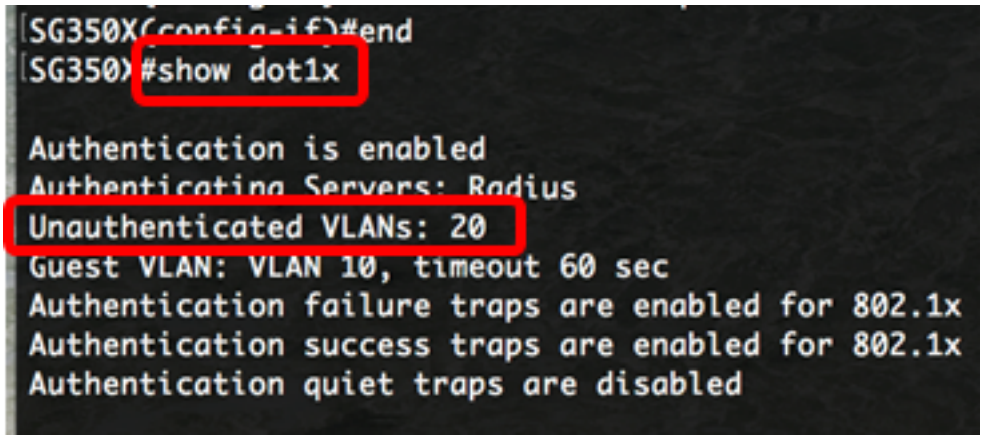
Step 4. (Optional) To enable 802.1x authentication on the VLAN, enter the following:

SG350X(config-if)#no dot1x auth-not-req

Step 5. To exit the Interface Configuration context, enter the following:



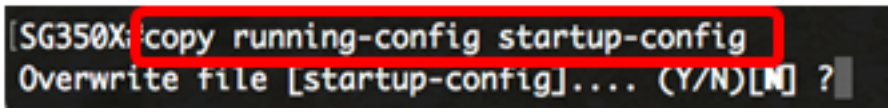
Step 6. (Optional) To display the 802.1x global authentication settings on the switch, enter the following:



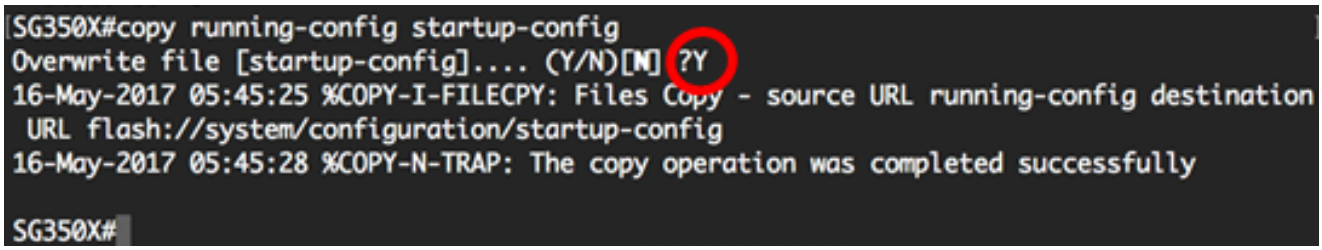
Note: In this example, VLAN 20 shows as an unauthenticated VLAN.

Step 7. (Optional) In the Privileged EXEC mode of the switch, save the configured settings to the startup configuration file, by entering the following:

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



Step 8. (Optional) Press **Y** for Yes or **N** for No on your keyboard once the Overwrite file [startup-config]… prompt appears.



You should now have successfully configured the 802.1x authentication settings on the VLANs on your switch.

Important: To proceed with configuring the 802.1x port authentication settings on your switch, follow the guidelines above.