Configure 802.1x Supplicant Credentials on a Switch

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 Area 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).

The 802.1x authentication restricts unauthorized clients from connecting to a LAN through publicly-accessible ports. The 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.

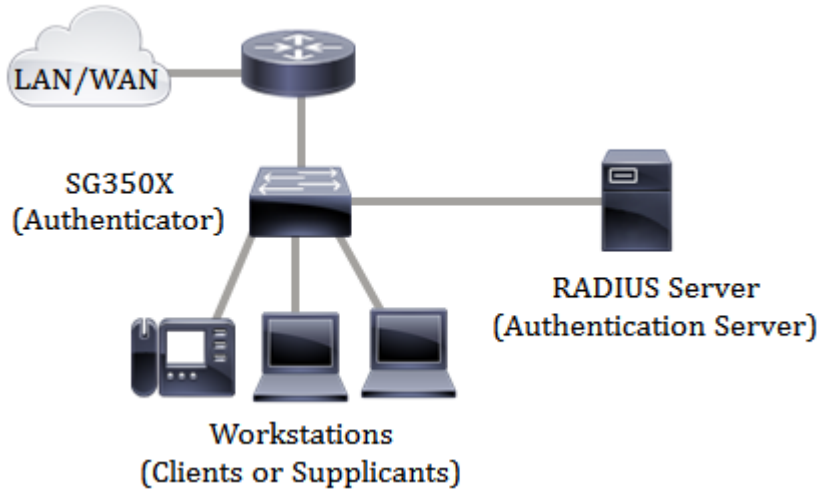
  - MAC-based — Supported in all authentication modes. With Media Access Control (MAC)-based, the authenticator itself executes the EAP client part of the software on behalf of the clients seeking network access.

  - 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.

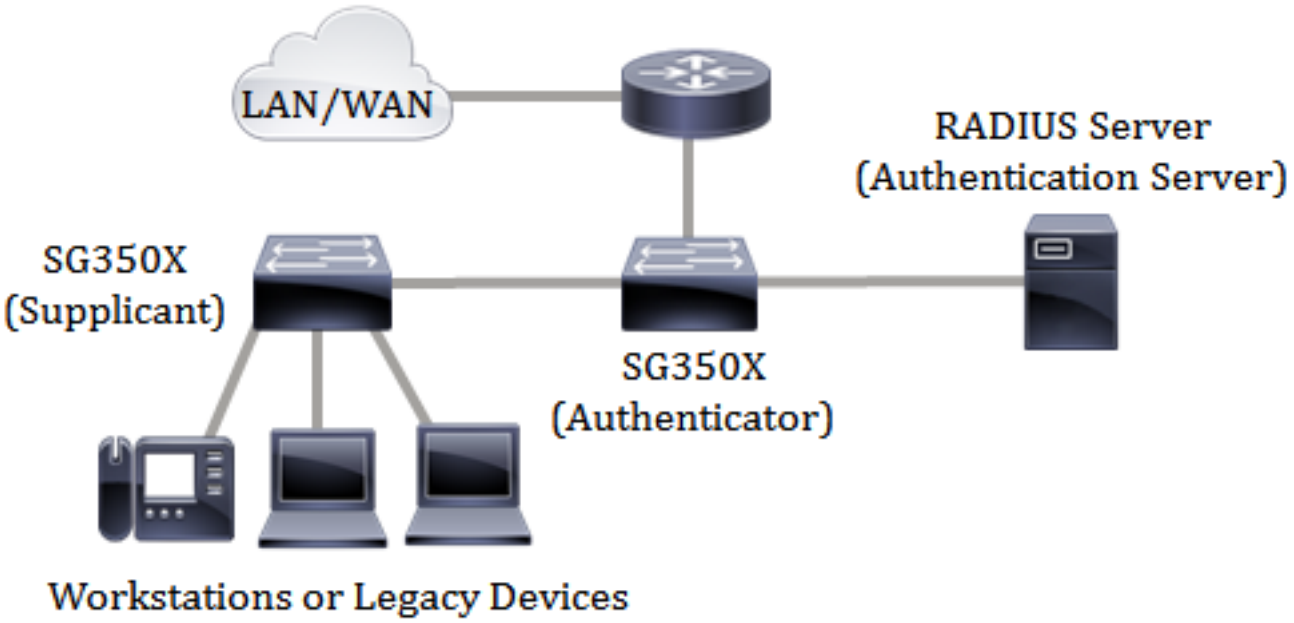
- Authentication server — An authentication server performs the actual authentication of the client. The authentication server for the device is a RADIUS authentication server with EAP extensions.

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.



However, you can also configure some ports on your switch as supplicants. Once the supplicant credentials are configured on a specific port on your switch, you can directly connect the devices that are not 802.1x-capable so the devices would be able to access the secured network. The image below shows a scenario of a network that has configured a switch as a supplicant.



Prerequisites in configuring 802.1x:

- Configure the RADIUS server. To learn how to configure the RADIUS server settings on your switch, click here.
- Create a Virtual Local Area Network (VLAN). To create VLANs using the web-based utility of your switch, click here. For CLI-based instructions, click here.
- Configure Port to VLAN settings on your switch. To configure using the web-based utility, click here. To use the CLI, click here.
- 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. For CLI-based instructions, click here.
- (Optional) Configure Time Range on the switch. To learn how to configure time range settings on your switch, click here. To use the CLI, click here.
- Configure 802.1x supplicant credentials on the switch. The instructions are provided in this article. For CLI-based instructions, click here.

- Configure 802.1x Port Authentication. To use the web-based utility of the switch, click here. To use the CLI, click here.

Objective

You can configure the switch as an 802.1x supplicant (client) on the wired network. An encrypted user name and password can be configured to allow the switch to authenticate using 802.1x.

On the networks that use IEEE 802.1x port-based network access control, a supplicant cannot gain access to the network until the 802.1x authenticator grants access. If your network uses 802.1x, you must configure 802.1x authentication information on the switch so that it can supply the information to the authenticator.

This article provides instructions on how to configure 802.1x supplicant credentials on your switch.

Applicable Devices

- Sx350X Series
- SG350X Series
- SG550X Series

Software Version

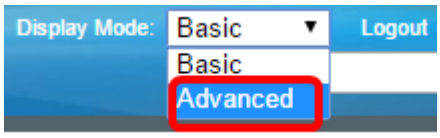
- 2.3.0.130

Configure 802.1x Supplicant Credentials

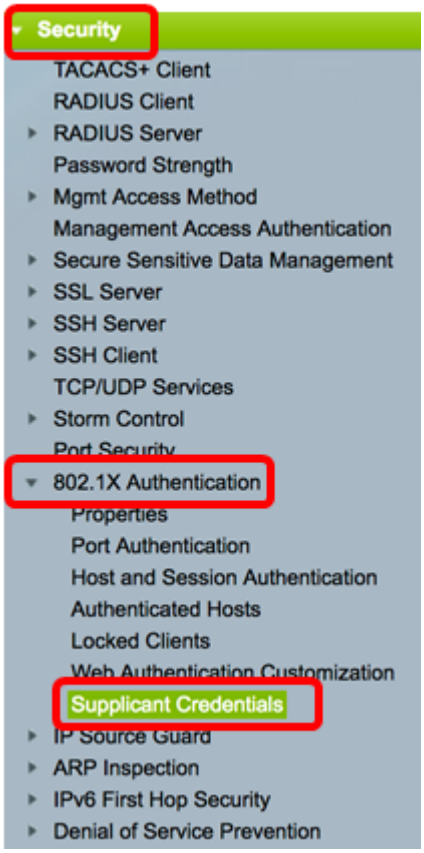
Create 802.1x Supplicant Credentials

Step 1. Log in to the web-based utility of your switch then choose **Advanced** in the Display Mode drop-down list.

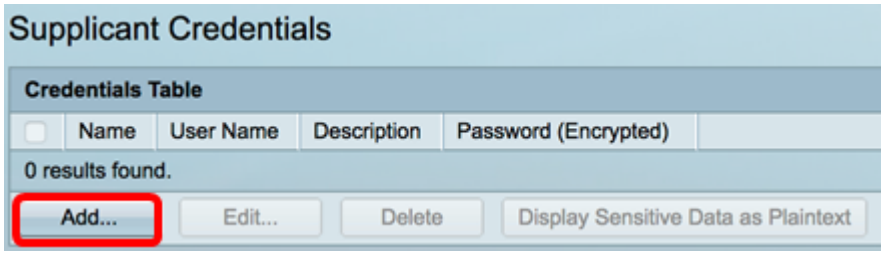
Note: The available menu options may vary depending on the device model. In this example, SG350X-48MP is used.



Step 2. Choose **Security > 802.1X Authentication > Supplicant Credentials**.



Step 3. Click the **Add** button to add new user credentials for the supplicant.



Step 4. Enter the credential name in the *Credential Name* field.

Note: In this example, cisco is entered.

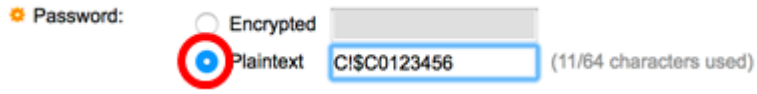
Step 5. In the *User Name* field, enter the username to associate with the credential name.

Note: In this example, switchuser is used.

Step 6. (Optional) Enter the description of the credential in the *Description* field.

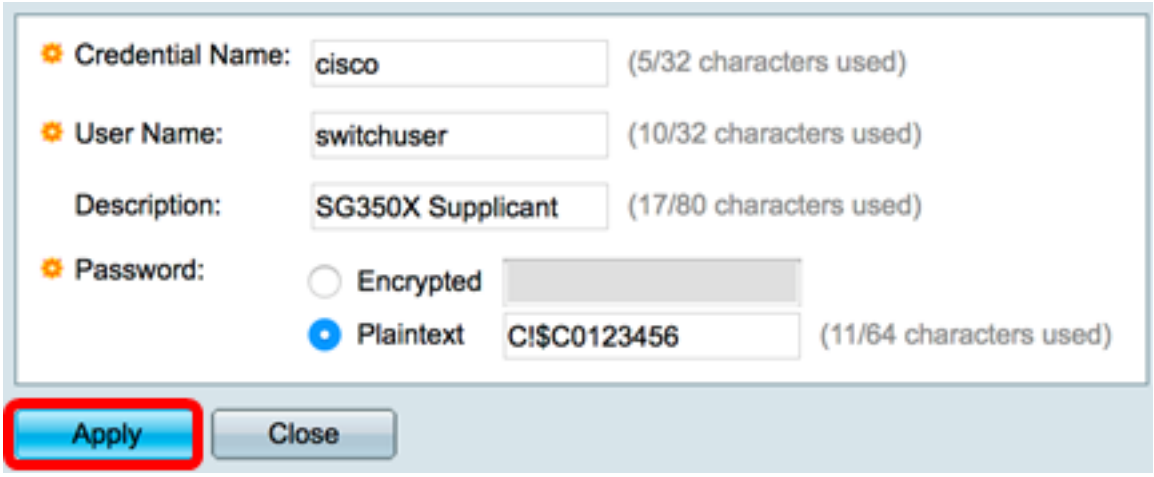
Note: In this example, SG350X Supplicant is used.

Step 7. Click the radio button that corresponds the type of password that you want to use then enter the password in the allocated field.



Note: In this example, Plaintext is chosen and the password used is C!$C0123456.

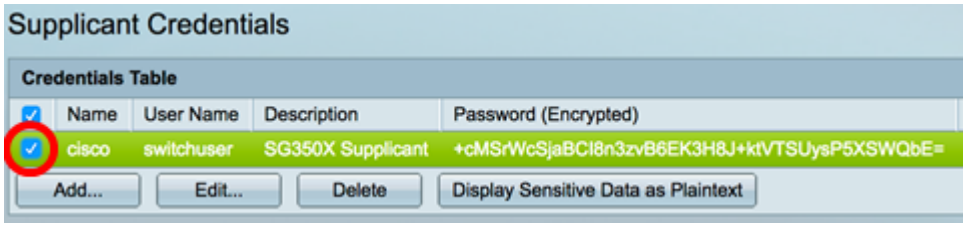
Step 8. Click **Apply** then click **Close**.



Step 9. (Optional) Click the **Save** button to save the settings to the startup configuration file.

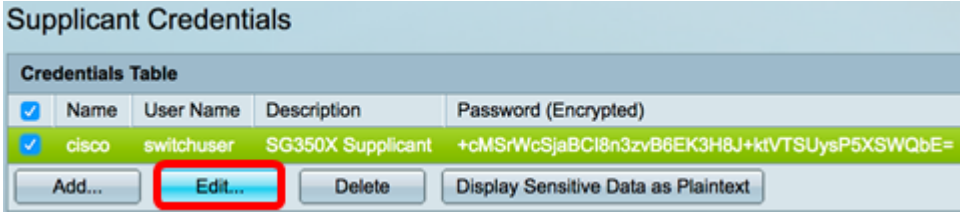
Edit an 802.1x Supplicant Credential

Step 1. Click the check box of the corresponding credential name that you want to edit.



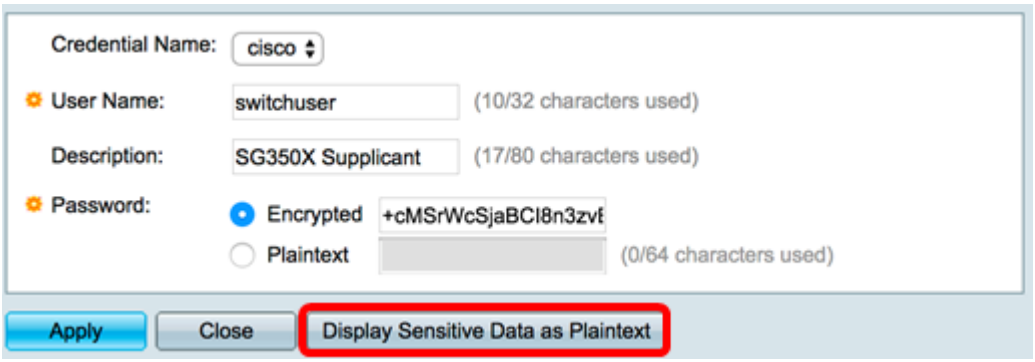
Note: In this example, cisco is chosen.

Step 2. Click the **Edit** button.

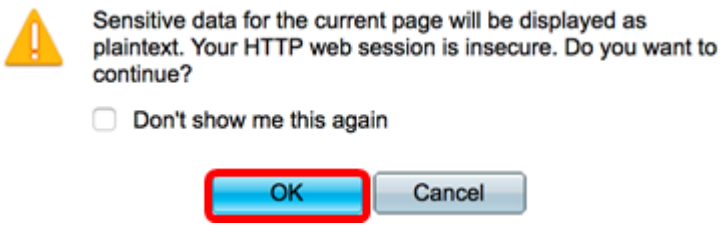


Step 3. (Optional) To display the encrypted password as plain text, click the **Display**

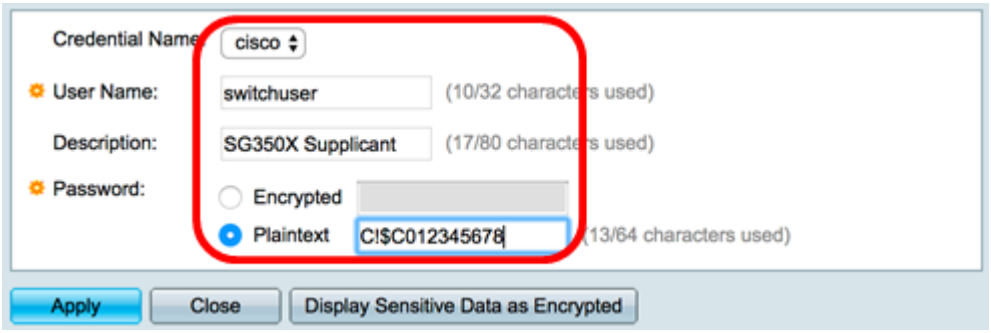
Sensitive Data as Plaintext button.



Step 4. (Optional) Click **OK** to display encrypted password as plaintext.

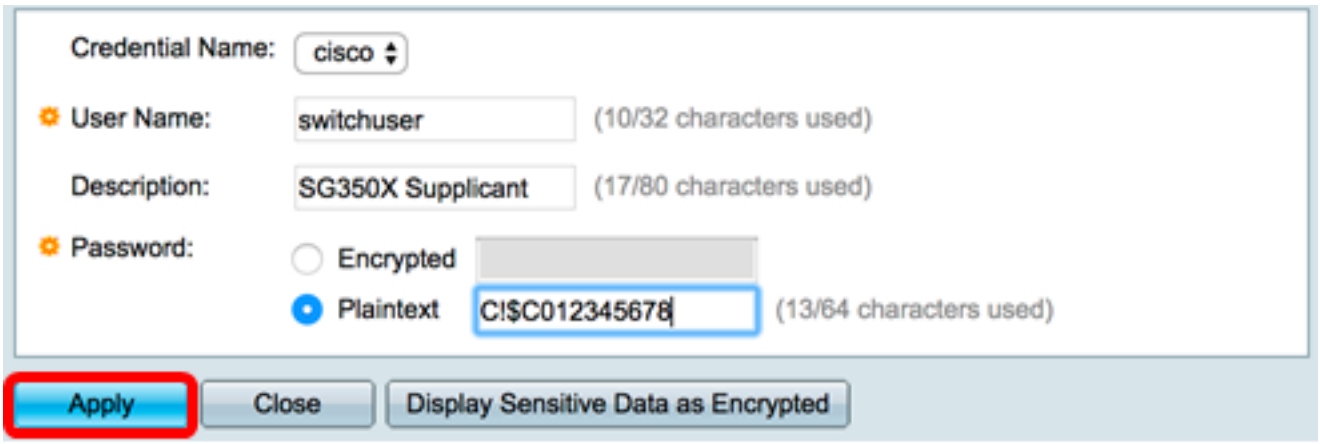


Step 5. Update the credential details accordingly.

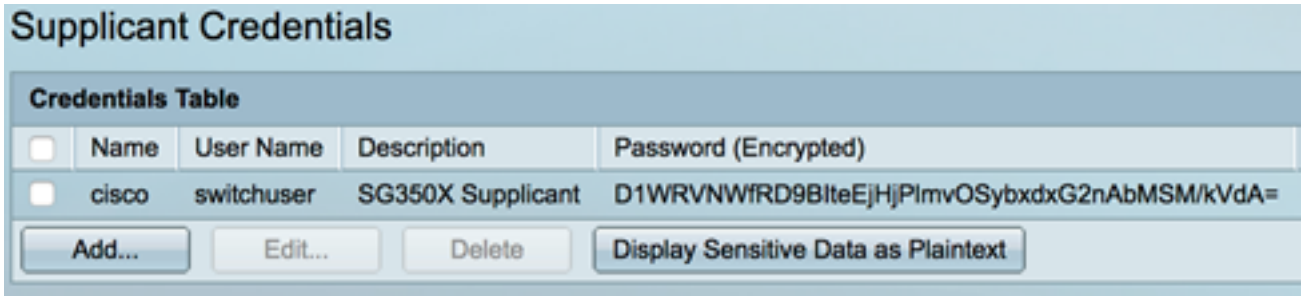


Note: In this example, the password is updated to C!$C012345678.

Step 6. Click **Apply** then click **Close**.



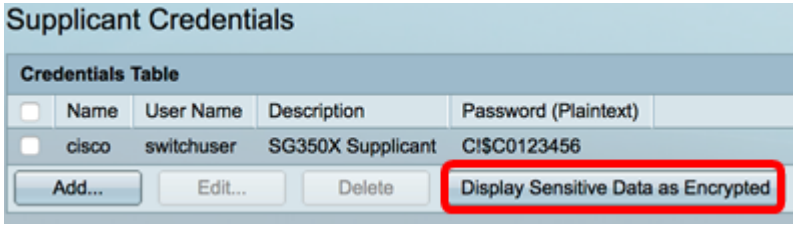
You should now have successfully edited the supplicant credential details on your switch.



Display Encrypted Password as Plaintext

Step 1. To display the encrypted password as plain text, click the **Display Sensitive Data as Plaintext** button.

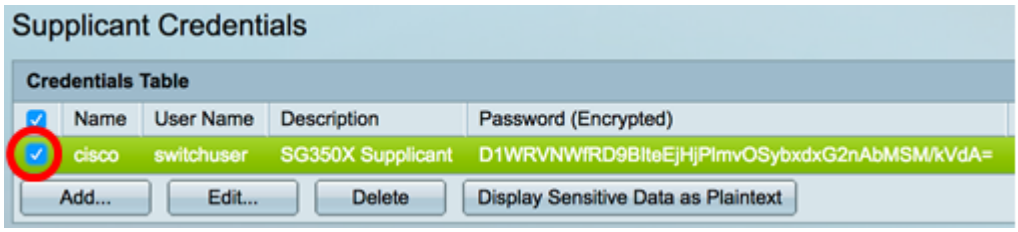
Step 2. (Optional) The password will be displayed in plaintext form. Click the **Display Sensitive Data as Encrypted** button to display the encrypted form of the password.



You should now have successfully displayed the sensitive password as plaintext.

Delete an 802.1x Supplicant Credential

Step 1. Click the check box of the corresponding credential name that you want to delete.



Step 2. Click the **Delete** button.

You should now have successfully deleted an entry from the Supplicant Credentials Table of

your switch.

Configure an 802.1x Supplicant Interface

To apply the configured 802.1x supplicant credentials, you must configure 802.1x authentication information on the switch so that it can supply the information to the authenticator. Refer to the prerequisites above to configure the 802.1x port authentication on your switch.