Configuring MAC-Based Authentication on a Switch

Objective

802.1X is an administration tool to whitelist devices, ensuring no unauthorized access to your network. This document shows you how to configure MAC-based authentication on a switch using the Graphical User Interface (GUI).

Note: This guide is lengthy at 9 sections and 1 section to verify a host has been authenticated. Grab coffee, tea or water and ensure you have ample time to review and execute the steps involved. To configure MAC-based authentication using the Command Line Interface (CLI), click here.

How Does Radius Work?

There are three main components to 802.1X authentication, a supplicant (client), an authenticator (network device such as a switch), and an authentication server (RADIUS). The Remote Authentication Dial-In User Service (RADIUS) is an access server that uses authentication, authorization, and accounting (AAA) protocol that help manage network access. RADIUS uses a client-server model in which secure authentication information is exchanged between the RADIUS server and one or more RADIUS clients. It validates the identity of the client and notifies the switch whether or not the client is authorized to access the LAN.

An authenticator works between the client and the authentication server. First, it will request identity information from the client. In response, the authenticator would verify the information with the authentication server. Lastly, it would relay a response to the client. In this article, the authenticator would be a switch that includes the RADIUS client. The switch would be able to encapsulate and decapsulate the Extensible Authentication Protocol (EAP) frames to interact with the authentication server.

What about MAC-Based Authentication?

In MAC-based authentication, when the supplicant does not understand how to talk to the authenticator or is unable to, it uses the MAC address of the host to authenticate. MAC-based supplicants are authenticated using pure RADIUS (without using EAP). The RADIUS server has a dedicated host database that contains only the allowed MAC addresses. Instead of treating the MAC-based Authentication request as a Password Authentication Protocol (PAP) authentication, the servers recognize such a request by Attribute 6 [Service-Type] = 10. They will compare the MAC address in the Calling-Station-Id attribute to the MAC addresses stored in the host database.

Version 2.4 release adds the ability to configure the format of the username sent for MAC-based supplicants and be defined either EAP authentication method or pure RADIUS. In this version, you can also configure the format of the username as well as configuring a specific password, different from username, for MAC-based supplicants.

Topology:
Note: In this article, we will be using the SG550X-24 for both the RADIUS server and the authenticator. The RADIUS server has a static IP address of 192.168.1.100 and the authenticator has a static IP address of 192.168.1.101.

The steps in this document are performed under the Advanced display mode. To change the mode to advanced, go to the top right corner and select Advanced in the Display Mode dropdown list.

Table of Content

1. RADIUS Server Global Settings
2. RADIUS Server Keys
3. RADIUS Server Groups
4. RADIUS Server Users
5. RADIUS Client
6. 802.1X Authentication Properties
7. 802.1X Authentication MAC-Based Authentication Settings
8. 802.1X Authentication Host and Session Authentication
9. 802.1X Authentication Port Authentication
10. Conclusion

Applicable Devices
Sx350X Series
SG350XG Series
Sx550X Series
SG550XG Series

Software Version

- 2.4.0.94

RADIUS Server Global Settings

Step 1. Log in to the web-based utility of your switch that will be configured as RADIUS server and navigate to Security > RADIUS Server > RADIUS Server Global Settings.

Step 2. To enable the RADIUS server feature status, check the Enable checkbox in the RADIUS Server Status field.

Step 3. To generate traps for RADIUS accounting events, logins that failed, or for logins that succeeded, check the desired Enable checkbox to generate traps. Traps are system events messages generated via Simple Network Management Protocol (SNMP). A trap is sent to the SNMP manager of the switch when a violation occurs. The following trap settings are:

- RADIUS Accounting Traps — Check to generate traps for RADIUS accounting events.
- RADIUS Authentication Failure Traps — Check to generate traps for logins that failed.
• RADIUS Authentication Success Traps — Check to generate traps for logins that succeeded.

Step 4. Click **Apply** to save your settings.

**RADIUS Server Keys**

Step 1. Navigate to **Security > RADIUS Server > RADIUS Server Keys**. The *RADIUS Server Key* page opens.

Step 2. In the *Secret Key Table* section, click **Add...** to add a secret key.
Step 3. The Add Secret Key window page opens. In the NAS Address field, enter the address of the switch that is containing RADIUS client. In this example, we will be using the IP address 192.168.1.101 as our RADIUS client.

Step 4. Select one of the radio button that is used as a Secret Key. The following options are:

- Use default key — For specified servers, the device attempts to authenticate the RADIUS client by using the existing, default Key String.
- Encrypted — To encrypt communications by using Message-Digest Algorithm 5 (MD5), enter the key in encrypted form.
- Plaintext — Enter the key string in plaintext mode.

In this example, we will be selecting Plaintext and using the word example as our Secret Key. After pressing apply, your key will be in an encrypted form.

Note: We do not recommend using the word example as the secret key. Please use a stronger key. Up to 128 characters can be used. If your password is too complex to remember then it's a good password, but even better if you can turn the password into a memorable passphrase with special characters and numbers replacing vowels — "P@55w0rds@reH@rdT0Remember". It is best to not use any word that can be found in a dictionary. It is best to choose a phrase and swap out some of the letters for special characters and numbers. Please refer to this Cisco blog post for more details.
Step 5. Click **Apply** to save your configuration. The secret key is now encrypted with MD5. MD5 is a cryptographic hash function that takes a piece of data and create a unique hexadecimal output that is typically not reproducible. MD5 uses a 128 bit hash value.

### RADIUS Server Keys

- **Default Key:**
  - Keep existing default key
  - Encrypted
  - Plaintext

- **MD5 Digest:**

  - **Apply**
  - **Cancel**

### Secret Key Table

- **NAS Address:** 192.168.1.101
- **Secret Key's MD5:** 1a79a4d60de6718e8e5b326e338ae533

  - **Add...**
  - **Edit...**
  - **Delete**

### RADIUS Server Groups

Step 1. Navigate to **Security > RADIUS Server > RADIUS Server Groups**.

Step 2. Click **Add...** to add a new RADIUS server group.
Step 3. The Add RADIUS Server Group page opens. Enter a name for the group. In this example, we will be using MAC802 as our group name.

Step 4. Enter the management access privilege level of the group in the Privilege Level field. The range is from 1 — 15, 15 being the most privileged and the default value is 1. In this example, we will be leaving the privilege level as 1.

Note: We will not be configuring Time Range or VLAN in this article.
Step 5. Click **Apply** to save your settings.

**RADIUS Server Users**

Step 1. Navigate to **Security > RADIUS Server > RADIUS Server Users** to configure users for RADIUS.

Step 2. Click **Add...** to add a new user.

Step 3. The **Add RADIUS Server User** page opens. In the **User Name** field, enter in the MAC address of a user. In this example, we will be using our Ethernet MAC address on our computer.

**Note:** A portion of the MAC address has been blurred out.
Step 4. Select a group in the Group Name drop-down list. As highlighted in step 3 of RADIUS Server Group section, we will be selecting MAC802 as our Group Name for this user.

Step 5. Select one of following radio buttons:

- Encrypted — A key is used to encrypt communications by using MD5. To use encryption, enter the key in encrypted form.
- Plaintext — If you do not have an encrypted key string (from another device), enter the key string in plaintext mode. The encrypted key string is generated and displayed.

We will be selecting Plaintext as our password for this user and typing in example as our plaintext password.

Note: It is not recommended to use example as the plaintext password. We recommend using a stronger password.
Step 6. Click **Apply** once you are done configuring.

Now you have finished configuring the RADIUS server. In the next section, we will be configuring the second switch to be an authenticator.

**RADIUS Client**

Step 1. Log in to the web-based utility of your switch that will be configured as the authenticator and navigate to **Security > RADIUS Client**.

Step 2. Scroll down to **RADIUS Table** section, then click **Add...** to add a RADIUS server.
Step 3. (Optional) Select whether to specify the RADIUS server by IP address or name in the **Server Definition** field. In this example, we will keep the default selection of **By IP address**.

Step 4. (Optional) Select the version of the IP address of the RADIUS server in the **IP Version** field. We will be keeping the default selection of **Version 4** for this example.

Step 5. Enter in the RADIUS server by IP address or name. We will be entering the IP address of **192.168.1.100** in the **Server IP Address/Name** field.
Step 6. Enter the priority of the server. The priority determines the order the device attempts to contact the servers to authenticate a user. The device starts with the highest priority RADIUS server first. Zero is the highest priority.

Step 7. Enter the key string used for authenticating and encrypting communication between the device and the RADIUS server. This key must match the key configured on the RADIUS server. It can be entered in **Encrypted** or **Plaintext** format. If **Use Default** is selected, the device attempts to authenticate to the RADIUS server by using the default Key String. We will be using the **User Defined (Plaintext)** and entering in the key example.

**Note:** We will be leaving the rest of the configuration as default. You may configure them if you like.
Step 8. Click **Apply** to save the configuration.

### 802.1X Authentication Properties

The properties page is used to globally enable port/device authentication. For authentication to function, it must be activated both globally and individually on each port.

**Step 1.** Navigate to **Security > 802.1X Authentication > Properties**.

**Step 2.** Check the **Enable** checkbox to enable port-based authentication.
Step 3. Select the user authentication methods. We will be choosing RADIUS as our authentication method. The following options are:

- **RADIUS, None** — Perform port authentication first by using the RADIUS server. If no response is received from RADIUS (for example, if the server is down), then no authentication is performed, and the session is permitted. If the server is available but the user credentials are incorrect, access is denied and the session terminated.
- **RADIUS** — Authenticate the user on the RADIUS server. If no authentication is performed, the session is not permitted.
- **None** — Do not authenticate the user. Permit the session.
Step 4. (Optional) Check the Enable check box for **MAC Authentication Failure Traps** and **MAC Authentication Success Traps**. This will generate a trap if MAC authentication fails or succeeds. In this example, we will enable both **MAC Authentication Failure Traps** and **MAC Authentication Success Traps**.

Step 5. Click **Apply**.

**802.1X Authentication MAC-Based Authentication Settings**
This page enables you to configure various setting applicable to MAC-based authentication.

Step 1. Navigate to **Security > 802.1X Authentication > MAC-Based Authentication Settings**.

Step 2. In the **MAC Authentication Type**, select one of the following:

- **EAP** — Use RADIUS with EAP encapsulation for the traffic between the switch (RADIUS client) and the RADIUS server, which authenticates a MAC-based supplicant.
- **RADIUS** — Use RADIUS without EAP encapsulation for the traffic between the switch (RADIUS client) and the RADIUS server, which authenticates a MAC-based supplicant.

In this example, we will be choosing RADIUS as our MAC authentication type.

Step 3. In the **Username Format**, select the number of ASCII characters between delimiters of the
MAC address sent as a user name. In this case, we will be choosing 2 as our group size.

**Note:** Make sure the username format is the same as the way you input the MAC address in *Radius Server Users* section.

Step 4. Select the character used as a delimiter between the defined groups of characters in the MAC address. In this example, we will select : as our group separator.
Step 5. In the Case field, select **Lowercase** or **Uppercase** to send the user name in lower or upper case.
Step 6. Password defines how the switch will use for authentication via the RADIUS server. Select one of the following options:

- Use default (Username) — Select this to use the defined username as the password.
- Encrypted — Define a password in encrypted format.
- Plaintext — Define a password in plaintext format.
Password Message-Digest Algorithm 5 (MD5) Digest displays the MD5 Digest password. MD5 is a cryptographic hash function that takes a piece of data and creates a unique hexadecimal output that is typically not reproducible. MD5 uses a 128 bit hash value.

Step 7. Click **Apply** and the settings are saved to the Running Configuration file.

**802.1X Authentication Host and Session Authentication**

The *Host and Session Authentication* page enables defining the mode in which 802.1X operates on the port and the action to perform if a violation has been detected.

Step 1. Navigate to **Security > 802.1X Authentication > Host and Session Authentication**.
Step 2. Select the port you want to configure host authentication. In this example, we will be configuring GE1 as it is connected to an end host.

Step 3. Click **Edit...** to configure the port.
Step 4. In the Host Authentication field, select one of the following options:

1. Single-Host Mode
   A port is authorized if there is an authorized client. Only one host can be authorized on a port. When a port is unauthorized and the guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless it belongs to the guest VLAN or to an unauthenticated VLAN. If a guest VLAN is not enabled on the port, only tagged traffic belonging to the unauthenticated VLANs is bridged. When a port is authorized, untagged and tagged traffic from the authorized host is bridged based on the static VLAN membership port configuration. Traffic from other hosts is dropped. A user can specify that untagged traffic from the authorized host will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. Tagged traffic is dropped unless it belongs to the RADIUS-assigned VLAN or the unauthenticated VLANs. Radius VLAN assignment on a port is set in the Port Authentication Page.

2. Multi-Host Mode
   A port is authorized if there is at least one authorized client. When a port is unauthorized and a guest VLAN is enabled, untagged traffic is remapped to the guest VLAN. Tagged traffic is dropped unless it belongs to the guest VLAN or to an unauthenticated VLAN. If guest VLAN is not enabled on a port, only tagged traffic belonging to unauthenticated VLANs is bridged. When a port is authorized, untagged and tagged traffic from all hosts connected to the port is bridged, based on the static VLAN membership port configuration. You can specify that untagged traffic from the authorized port will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. Tagged traffic is dropped unless it belongs to the RADIUS-assigned VLAN or the unauthenticated VLANs.
traffic is dropped unless it belongs to the RADIUS-assigned VLAN or to the unauthenticated VLANs. Radius VLAN assignment on a port is set in the Port Authentication page.

3. Multi-Sessions Mode Unlike the single-host and multi-host modes, a port in the multi-session mode does not have an authentication status. This status is assigned to each client connected to the port. Tagged traffic belonging to an unauthenticated VLAN is always bridged regardless of whether the host is authorized or not. Tagged and untagged traffic from unauthorized hosts not belonging to an unauthenticated VLAN is remapped to the guest VLAN if it is defined and enabled on the VLAN, or is dropped if the guest VLAN is not enabled on the port. You can specify that untagged traffic from the authorized port will be remapped to a VLAN that is assigned by a RADIUS server during the authentication process. Tagged traffic is dropped unless it belongs to the RADIUS-assigned VLAN or to the unauthenticated VLANs. Radius VLAN assignment on a port is set in the Port Authentication page.

![Port Authentication Interface](image)

Step 5. Click **Apply** to save your configuration.

**Note:** Use Copy Settings... to apply the same configuration of GE1 to multiple ports. Leave the port that is connected to the RADIUS server as **Multiple Host (802.1X)**.

### 802.1X Authentication Port Authentication

The Port Authentication page enables configuration of parameters for each port. Since some of the configuration changes are only possible while the port is in Force Authorized state, such as host authentication, it is recommended that you change the port control to Force Authorized before making changes. When the configuration is complete, return the port control to its previous state.

**Note:** We will only be configuring settings that is required for MAC-based authentication. The rest of the configuration will be left as default.

Step 1. Navigate to **Security > 802.1X Authentication > Port Authentication**.
Step 2. Select the port that you want to configure port authorization.

**Note:** Do not configure the port that the switch is connected to. The switch is a trusted device so leave that port as **Forced Authorized**.

Step 3. Then scroll down and click **Edit...** to configure the port.

In the **Edit Port Authentication** page, the **Current Port Control** field displays the current port authorization state. If the state is **Authorized**, the port is either authenticated or the **Administrative Port Control** is **Force Authorized**. Conversely, if the state is **Unauthorized**, then the port is either not authenticated or the **Administrative Port Control** is **Force Unauthorized**. If supplicant is enabled on an interface, the current port control will be **Supplicant**.

Step 4. Select the administrative port authorization state. Configure the port to **Auto**. The available
options are:

- **Forced Unauthorized** — Denies the interface access by moving the interface into the unauthorized state. The device does not provide authentication services to the client through the interface.
- **Auto** — Enables port-based authentication and authorization on the device. The interface moves between an authorized or unauthorized state based on the authentication exchange between the device and the client.
- **Forced Authorized** — Authorizes the interface without authentication.

**Note:** *Forced Authorized* is the default value.

Step 5. In the **802.1X Based Authentication** field, uncheck the **Enable** checkbox as we are not going to use 802.1X as our authentication. The default value of **802.1x Based Authentication** is enabled.

Step 6. Check the **Enable** checkbox for **MAC Based Authentication** as we want to enable port authentication based on the supplicant MAC address. Only 8 MAC-based authentications can be used on the port.
Step 7. Click **Apply** to save your changes.

If you want to save your configuration, press the **Save** button at the top of your screen.

**Conclusion**

You have now successfully configured MAC-based authentication on your switch. To verify that the MAC-based authentication is working, follow the steps below.

Step 1. Navigate to **Security > 802.1X Authentication > Authenticated Hosts** to view details about authenticated users.

Step 2. In this example, you can see our Ethernet MAC address was authenticated in the **Authenticated Host Table**. The follow fields defines as:

- **User Name** — Supplicant names that authenticated on each port.
- **Port** — Number of the port.
- **Session Time (DD:HH:MM:SS)** — Amount of time that the supplicant was authenticated and authorized access at the port.
- **Authentication Method** — Method by which the last session was authenticated.
- **Authenticated Server** — RADIUS server.
- **MAC Address** — Displays the supplicant MAC address.
- **VLAN ID** — Port's VLAN.
Step 3. (Optional) Navigate to **Status and Statistics > View Log > RAM Memory**. The **RAM Memory** page will display all messages that saved in the RAM (cache) in chronological order. Entries are stored in the RAM log according to the configuration in the Log Settings page.

Step 4. In the **RAM Memory Log Table**, you should see an informational log message that states your MAC address being authorized on port gi1/0/1.

**Note**: Part of the MAC address is blurred out.