



App note on MAC-address based SSID restriction

About	1
System Requirements.....	3
Controller Configuration.....	3
To Configure RADIUS profile	3
Enable Mac-filtering globally	4
To Configure Security profile.....	5
To Configure ESS profile.....	6
IDM Configuration.....	7
Create Authorization Profiles for Students and Staff.....	7
Configure an Authorization Policy	8
Configure device accounts from IDM sponsor interface.....	9

About

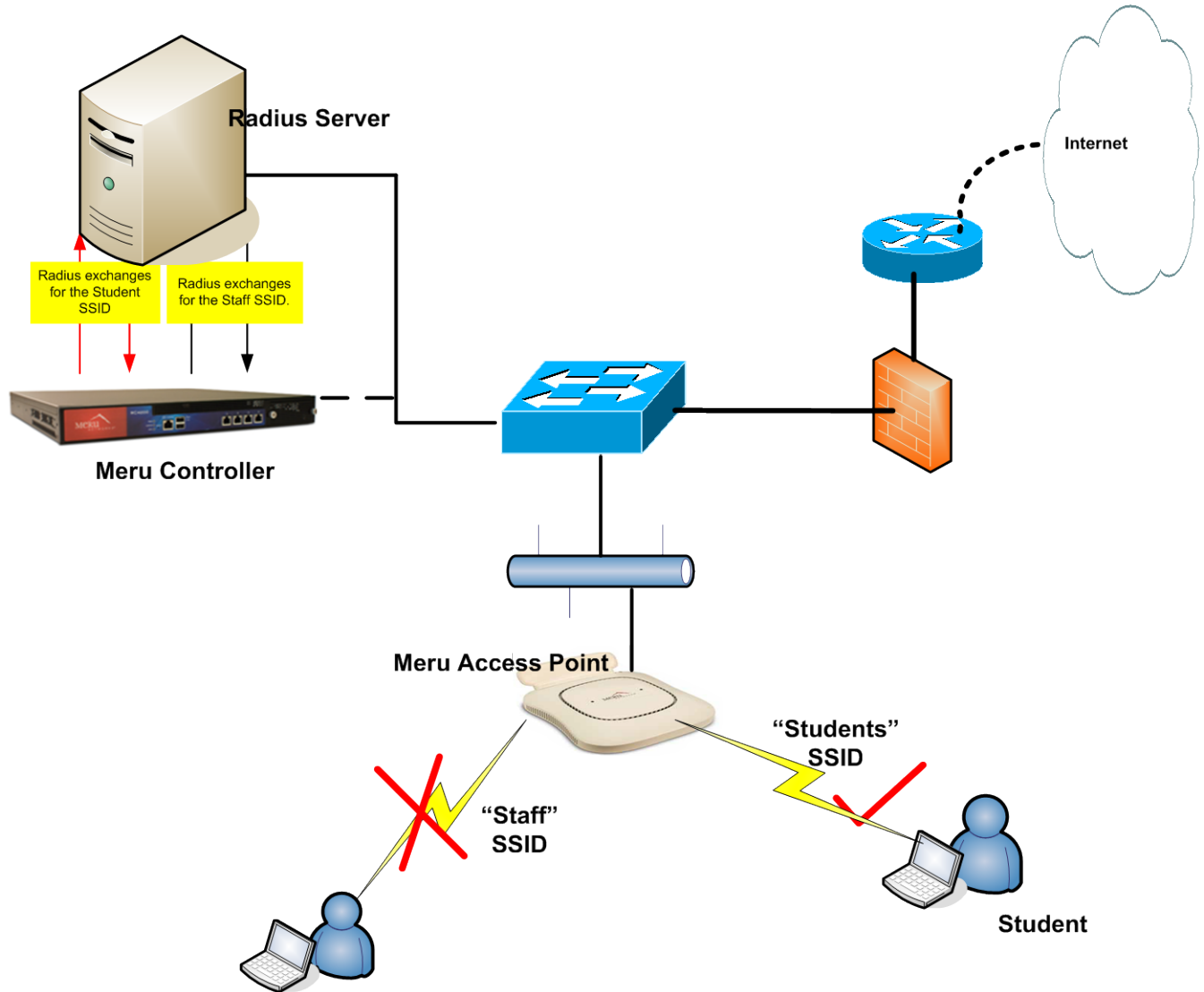
MAC-address authentication with SSID information in a RADIUS request (in compliance with RFC3580) can be configured in Meru controllers starting from System Director (SD) version 6.0. The called-station-id attribute in a RADIUS request will have the SSID appended to it, in the following format 00-0B-2D-48-20-F9: Student, where the MAC-address is of the 802.1x authenticator which is the controller in a Meru WLAN.

By configuring the controller to append the SSID to the MAC address the RADIUS server can respond correctly to grant or deny access for a station based on its SSID.

[Figure 1](#) illustrates the Network Diagram and Use case

The MAC-addresses of the devices used by staff and students are registered in the network directory which the RADIUS server uses to authenticate. These MAC-addresses are configured to be part of separate groups. When an access request from a client with the wrong SSID or an SSID which it's not supposed to join, reaches the RADIUS server, the access request is rejected. In this example the rule is set to reject the Student devices authenticating against the Staff SSID.

Figure 1: Network Diagram



System Requirements

To configure MAC authentication with SSID restriction, you need the following system requirements:

- System Director Release 6.0 or later
- Any Meru Controller models



There are no differences between physical or virtual controller models in the way this feature works. This document describes the configuration tasks on controller and IDM which is the RADIUS server.

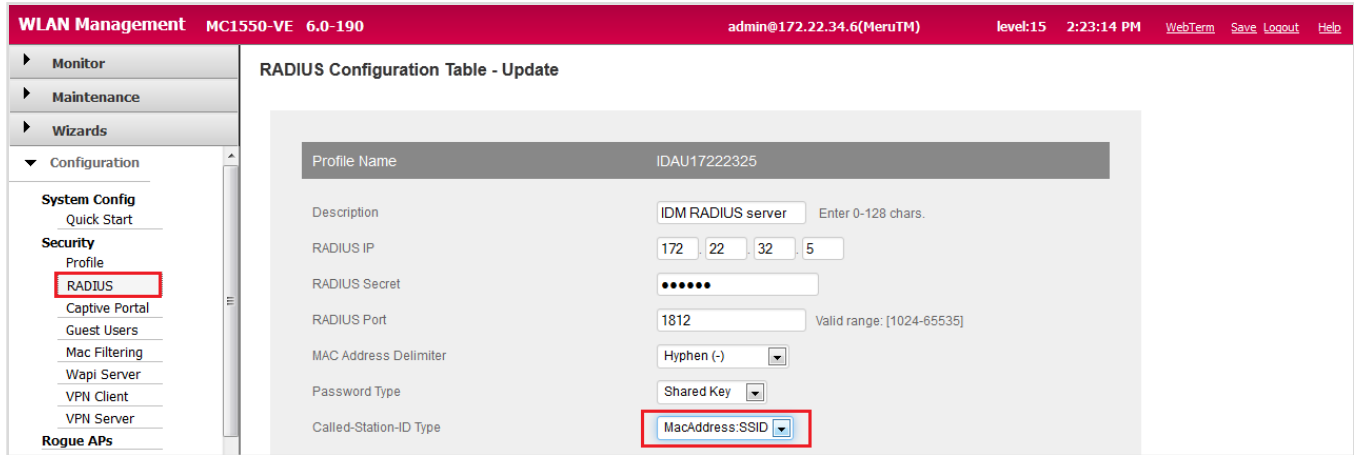
Controller Configuration

- [Configure RADIUS profile](#)
- [Enable Mac-Filtering Globally and map the RADIUS Profile](#)
- [Create a Security Profile and enable the mac-filtering flag](#)
- [Create ESS profiles and map the Security Profile to each](#)

Configure RADIUS Profile

1. In the Web UI, click **Configuration > RADIUS**. (See [Figure 2](#))
2. Enter RADIUS description.
3. Enter RADIUS server IP address.
4. Enter RADIUS port (if different than default (1812)).
5. Select MAC address delimiter.
6. Select Password type.
7. Change Called-Station-ID Type to: "MacAddress:SSID".

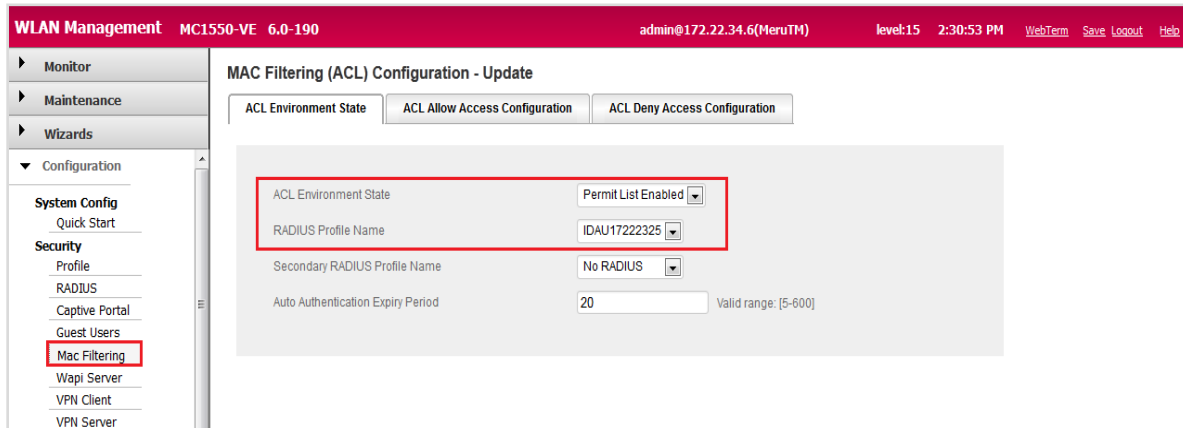
Figure 2: RADIUS Profile Configuration Page



Enable Mac-Filtering Globally

1. In the Web UI, click Configuration > MAC Filtering. (See [Figure 3](#)).
2. Enable the Permit List for the ACL Environment state.
3. Select the RADIUS profile in the RADIUS Profile name configuration tab.
4. Configure rest of the fields if required or leave it.

Figure 3: Enabling MAC Filtering



Configure Security Profile

1. In the Web UI, click Configuration > Security > Profile. (See [Figure 4](#)).
2. In L2 Modes Allowed select, Clear (Various security modes can also be used along with mac-filtering)
3. Set MAC Filtering flag to ON.

Figure 4: Security Profile Configuration Page

The screenshot displays the 'WLAN Management' web interface for an MC1550-VE device (version 6.0-190). The left sidebar shows a navigation menu with 'Profile' highlighted under the 'Security' section. The main content area is titled 'Security Profile Configuration' and contains the following settings:

- L2 Modes Allowed:** Clear, WPA, WPA2 PSK, WAI, 802.1x, WPA PSK, MIXED, WAI PSK, Static WEP keys, WPA2, MIXED_PSK.
- Data Encrypt:** WEP64, WEP128, TKIP, CCMP-AES, CCMP/TKIP, WPI-SMS4, Clear.
- Primary RADIUS Profile Name:** No RADIUS
- Secondary RADIUS Profile Name:** No RADIUS
- WEP Key (Alphanumeric/Hexadecimal):** [Empty field]
- Static WEP Key Index:** 1 (Valid range: [1-4])
- Re-Key Period (seconds):** 0 (Valid range: [0-65535])
- BKSA Caching Period (seconds):** 0 (Valid range: [0-65535])
- Captive Portal:** Disabled
- Captive Portal Authentication Method:** internal
- 802.1X Network Initiation:** OFF
- Tunnel Termination:** PEAP, TTLS
- Shared Key Authentication:** OFF
- Pre-shared Key (Alphanumeric/Hexadecimal):** [Empty field]
- Group Keying Interval (seconds):** 0 (Valid range: [0-65535])
- PMK Caching:** OFF
- Key Rotation:** Disabled
- Backend Auth Server Timeout:** 30 (Valid range: [1-65535])
- Reauthentication:** OFF
- MAC Filtering:** On
- Firewall Capability:** none

Buttons for 'OK' and 'Cancel' are located at the bottom right of the configuration area.

Configure ESS profile

1. In the Web UI, click **Configuration > ESS > Add**. (See [Figure 5](#)).
2. Type Profile name.
3. Select Enable from Enable/Disable dropdown.
4. Type SSID name.
5. Select the Security Profile created in [Configure Security Profile](#).
6. Click OK.

Figure 5: ESS Profile Configuration Page

The screenshot displays the 'ESS Profile - Add' configuration page. The left sidebar shows the navigation menu with 'Configuration' expanded and 'ESS' selected under 'Wireless'. The main content area contains the following fields:

Field	Value	Notes
ESS Profile	Staff	Enter 1-32 chars., Required
Enable/Disable	Enable	Dropdown menu
SSID	Staff	Enter 0-32 chars.
Security Profile	mac-authentication	Dropdown menu
Primary RADIUS Accounting Server	No RADIUS	Dropdown menu
Secondary RADIUS Accounting Server	No RADIUS	Dropdown menu
Accounting Interim Interval (seconds)	3600	Valid range: [600-36000]
Beacon Interval (msec)	100	Valid range: [20-1000]
SSID Broadcast	On	Dropdown menu
Bridging	<input type="checkbox"/> AirFortress <input type="checkbox"/> IPV6 <input type="checkbox"/> AppleTalk	Checkboxes
New AP's Join ESS	On	Dropdown menu
Tunnel Interface Type	No Tunnel	Dropdown menu
VLAN Name	No Data for VLAN Name	Text field
GRE Tunnel Profile Name	No Data for GRE Tunnel Profile Name	Text field
Allow Multicast Flag	Off	Dropdown menu
Isolate Wireless To Wireless traffic	Off	Dropdown menu
Multicast-to-Unicast Conversion	On	Dropdown menu

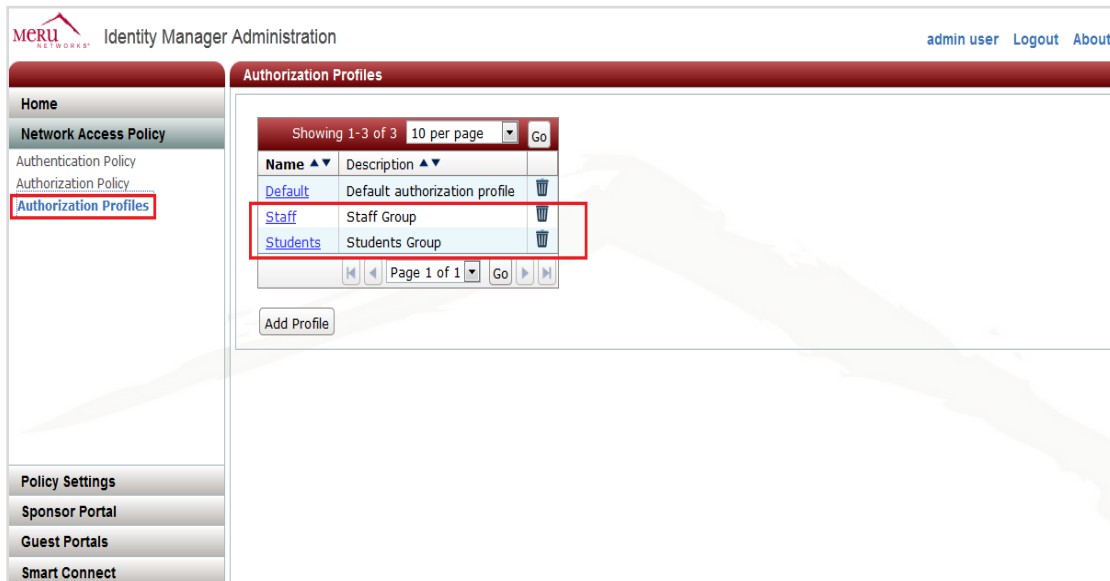
IDM Configuration

- [Create authorization profiles for Students and Staff](#)
- [Configure an authorization policy](#)
- [Add the MAC-address of various devices from the sponsor interface](#)

Create Authorization Profiles for Students and Staff

1. Under Network Access Policy select Authorization Profiles.
2. Click the Add Profile button.
3. Give a name and description to create an Authorization profile. Example: Profiles named Staff and Students in [Figure 6](#).

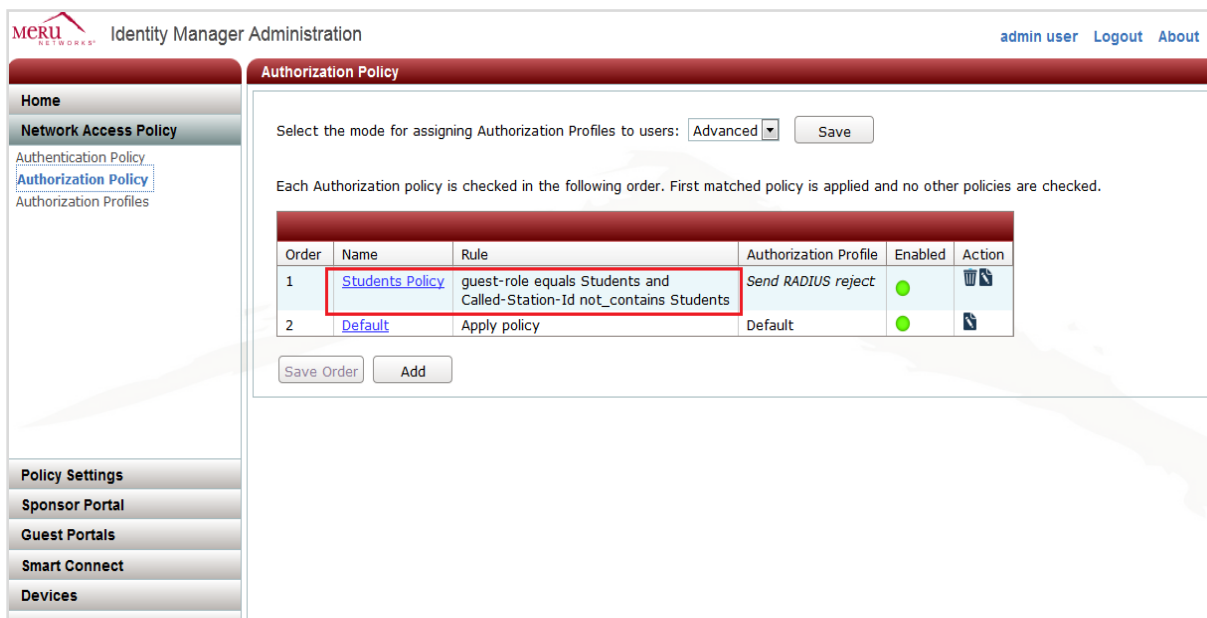
Figure 6: Configuring Authorization Profiles



Configure an Authorization Policy

1. Under Network Access Policy select Authorization Policy.
2. Select the advanced mode and click the Save button.
3. Click the Add button and navigate through authorization rule wizard by providing the appropriate name and description to the network policy.
4. While selecting the conditions, set the guest role to “Students” and click the “add condition” hyperlink. From the “Select Attribute” window, choose:
 - a. Type as “RADIUS”,
 - b. Vendor as “IETF”
 - c. Attribute as “called-station-id”
 - d. Click the set button
5. Configure a rule, if the called-station-id, "not contains", the string “Students”, return no access or access reject. See [Figure 7](#) for details.

Figure 7: An authorization policy to send RADIUS reject for requests that does not contain the required SSID






Meru Networks Identity Manager Administration admin user Logout About

Authorization Policy

Select the mode for assigning Authorization Profiles to users: Advanced Save

Each Authorization policy is checked in the following order. First matched policy is applied and no other policies are checked.

Order	Name	Rule	Authorization Profile	Enabled	Action
1	Students Policy	guest-role equals Students and Called-Station-Id not_contains Students	Send RADIUS reject	●	 
2	Default	Apply policy	Default	●	

Save Order Add

Configure Device Accounts from IDM Sponsor Interface

1. Open the IDM sponsor interface.
2. Select Create Accounts -> Create Device Account.
3. Add the device Mac-address and fill in the rest of the appropriate tabs. Select the Guest role as “Students” in this case. See [Figure 8](#) for details.

Figure 8: Creating Device Accounts from IDM sponsor Interface

The screenshot displays the Meru Identity Manager web interface for creating a device account. The browser's address bar is highlighted with a red box, showing the URL `https://172.22.32.5/sponsor`. The left-hand navigation menu is also visible, with the 'Create Device Account' option under the 'Create Accounts' section highlighted with a red box. The main content area, titled 'Create Device Account', contains the following form fields:

- MAC Address:
- First Name:
- Last Name:
- Company:
- Email Address:
- Mobile Phone Number:
- Guest Role:
- Time Profile:

At the bottom of the form, there are two buttons: 'Add User' and 'Cancel'.