

Troubleshoot Recent 802.1X Failure Alert in Meraki Device

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Problem](#)

[What is the RADIUS test in Meraki devices?](#)

[Configure](#)

[Network Diagram](#)

[Verify And Troubleshoot](#)

[802.1X Configuration](#)

[802.1X Configuration Verification Test](#)

[Related Information](#)

[Note](#)

Introduction

This document describes how to resolve the recent 802.1X failure alert in the Meraki device.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Understand basic Meraki Software-Defined Wide Area Network (SDWAN) solution
- Understand basic Access Policy & Radius authentication

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

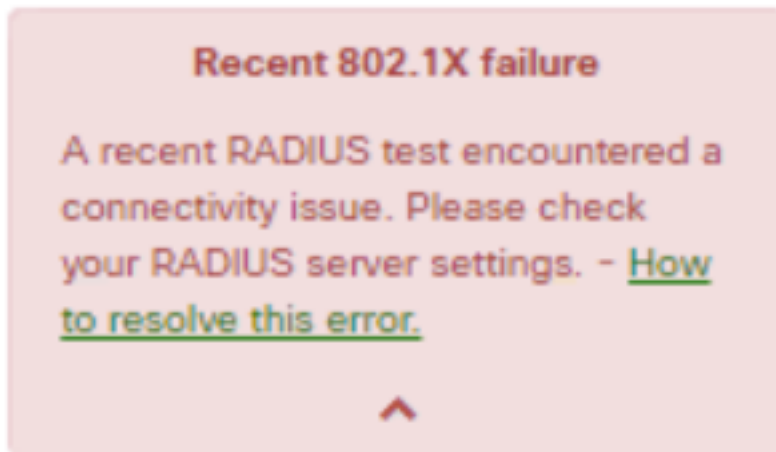
Problem

Meraki devices use the AAA radius server policy configuration to authenticate the end-user.

What is the RADIUS test in Meraki devices?

The recent 802.1X failure alert displayed that, if the periodic access-request messages sent to the configured RADIUS servers are unreachable, you must use a timeout period of 10 seconds.

Meraki devices periodically send Access-Request messages to the configured RADIUS servers that use identity **meraki_8021x_test** to ensure that the RADIUS servers are reachable. These Access-Requests have a timeout of 10 seconds and if the RADIUS server does not respond then it considers radius servers are unreachable and prompts the alert "Recent 802.1X failure" message. Refer to the screenshot of the alert seen on the device:



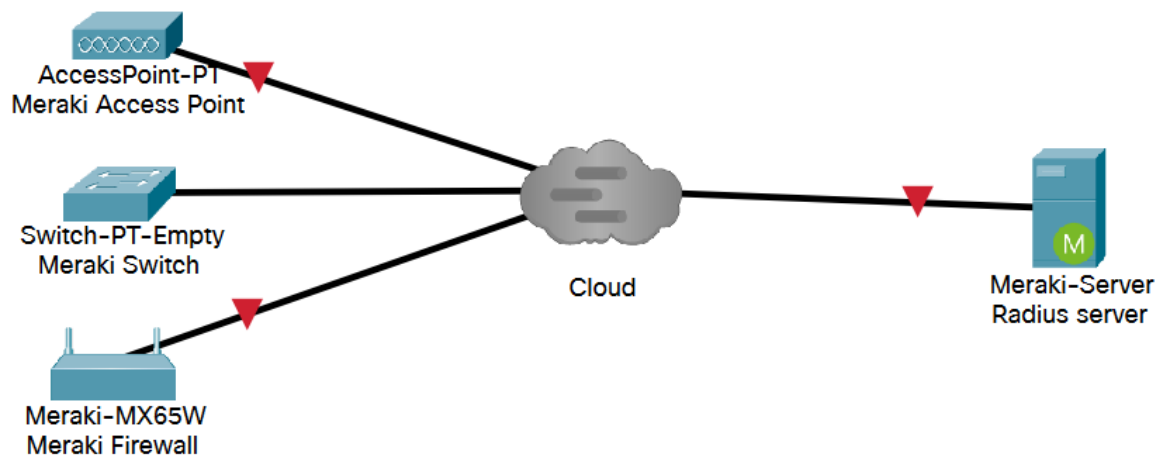
A test is considered successful if the Meraki device receives any legitimate RADIUS response (Access-Accept/Reject/Challenge) from the server.

With the RADIUS test enabled, all RADIUS servers are kept test run on every node at least once per 24 hours regardless of a test result. If a RADIUS test fails for a given node, it tests again every hour until a result that passes occurs. A subsequent pass marks the server reachable, clears the alert, and returns to the 24-hour test cycle.

Configure

Network Diagram

Here is a simple topology diagram that describes the setup:



Verify And Troubleshoot

802.1X Configuration

802.1X RADIUS configuration can be found in the path shown that depends on the Meraki product Model.

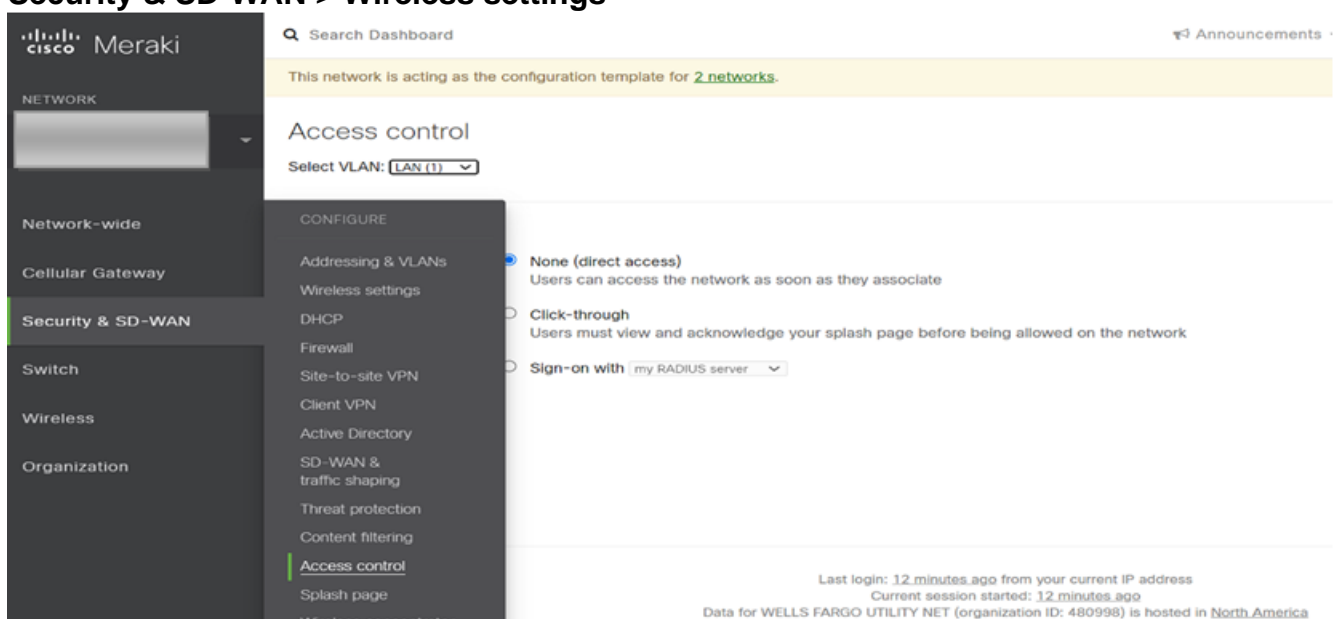
1. MX-Security appliance (configured either for access ports or wireless)

- For Access Ports

Security & SD-WAN > Addressing & VLANs

- For Wireless

Security & SD-WAN > Wireless settings



2. MR-Access points (enabled on a per Service Set Identifier (SSID) basis):

Wireless > Access control

Meraki

NETWORK

Small_Site

Network-wide

Security & SD-WAN

Switch

Wireless

Organization

CONFIGURE

SSIDs

Access control

Firewall & traffic shaping

Splash page

SSID availability

IoT radio settings

Port profiles

Radio settings

Hotspot 2.0

Air Marshal

RADIUS servers

#	Host	Port	Secret	Actions
1		1812	*****	⬇ ⬆ ⬇ × Test
2		1812	*****	⬇ ⬆ ⬇ × Test

[Add a server](#)

RADIUS testing [?]

RADIUS CoA support [?]

RADIUS attribute [?]

RADIUS accounting is enabled

#	Host	Port	Secret	Actions
1		1813	*****	⬇ ⬆ ⬇ ×
2		1813	*****	⬇ ⬆ ⬇ ×

[Add a server](#)

Do not use Meraki proxy

Disabled: do not assign group policies automatically

3. MS-Switches

Switch > Access Policies

Meraki

NETWORK

Small_Site

Network-wide

Security & SD-WAN

Switch

Wireless

Organization

CONFIGURE

Profiles

Profile ports

ACL

Access policies

Port schedules

Switch settings

Search Dashboard

Announcements

This network is acting as the configuration template for [231 networks](#).

Access policies

Name

Authentication method

RADIUS servers [?]

#	Host	Port	Secret	Actions
1		1812	*****	⬇ ⬆ ⬇ × Test
2		1812	*****	⬇ ⬆ ⬇ × Test

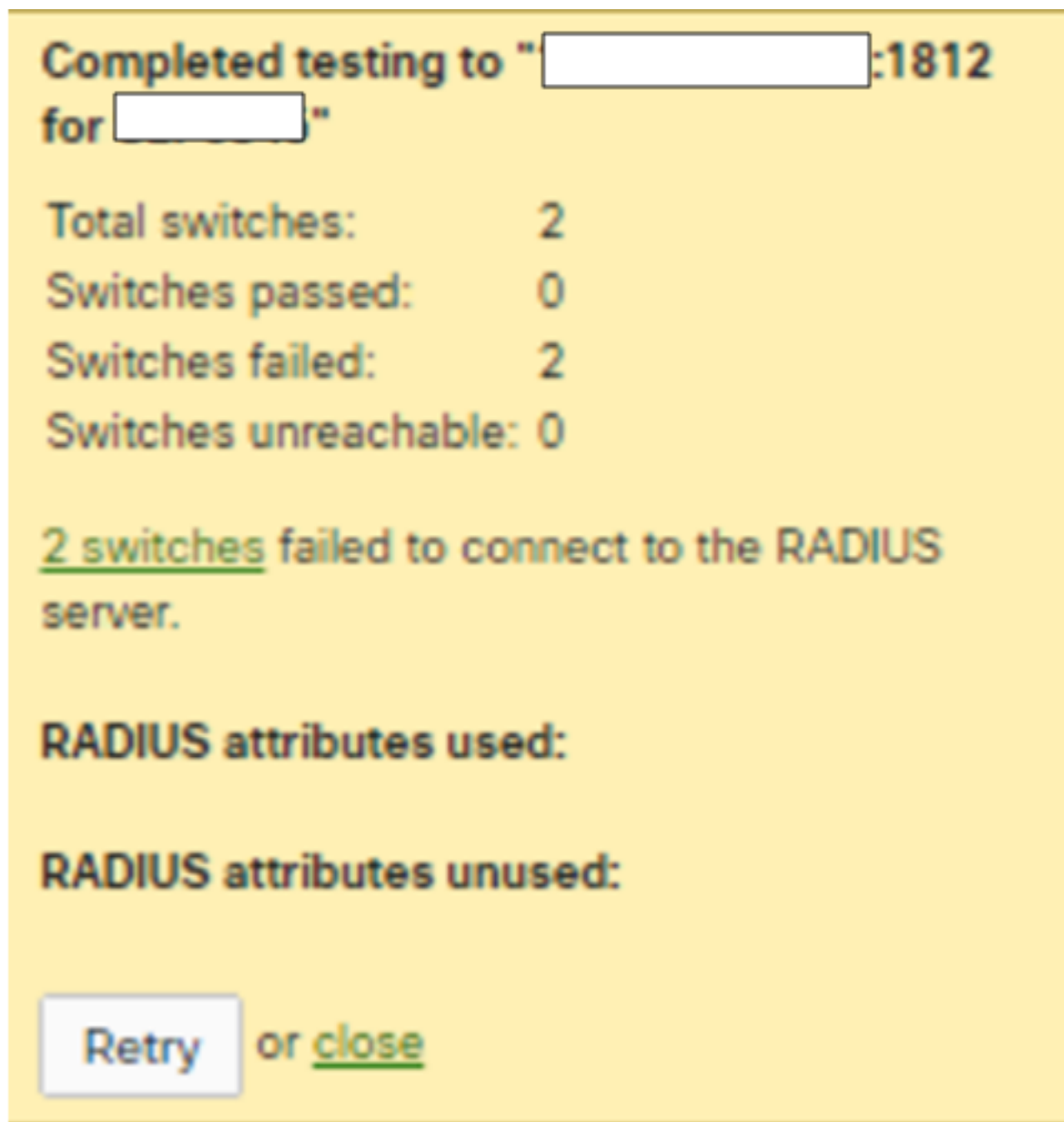
[Add a server](#)

#	Host	Port	Secret	Actions
1		1813	*****	⬇ ⬆ ⬇ × Test
2		1813	*****	⬇ ⬆ ⬇ × Test

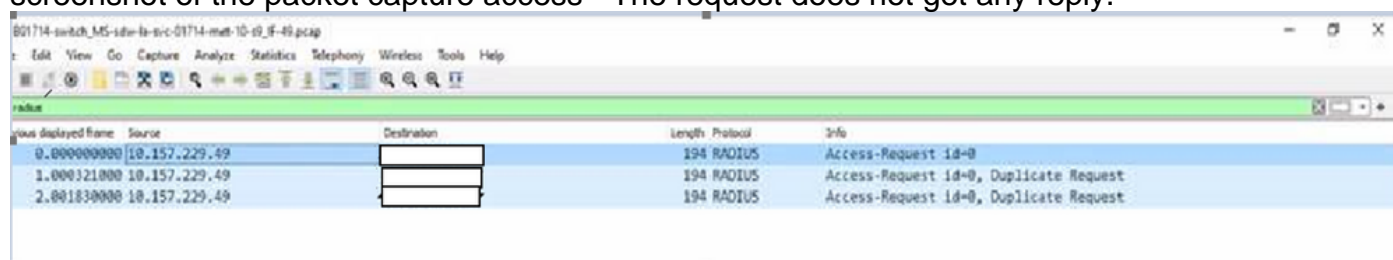
802.1X Configuration Verification Test

- Meraki Dashboard > Network Template > Switch > Access Policies > Radius Servers > Test
- Meraki Dashboard > Network Template > Wireless > Access Control > Radius Servers > Test

1. If the test result is noticed as **All AP failed to connect radius server**, you need to check where the access-Request got dropped.



2. Run the packet capture on the uplink port and verify the access-request flow. Refer to the screenshot of the packet capture access - The request does not get any reply.



3. If noticed test result gets replied as accept/reject/deny/response/incorrect credentials, it means the radius server is alive.

Completed testing to "[redacted]:1812 for
[redacted]"

Total APs: 1
APs passed: 0
APs failed: 1
APs unreachable: 0

Authentication failed while testing on one of your APs. This means the RADIUS server was reached but your credentials were incorrect. The test was stopped to prevent this account from being locked out due to multiple failed attempts. Please try again with different username and/or password.

RADIUS attributes used:

RADIUS attributes unused:

[Retry](#) or [close](#)

4. Run the packet capture on the uplink port and verify the access-request flow. Refer to the screenshot of the packet capture access - The request got a reply.

Source	Destination	Length	Protocol	Info
0.000000000 10.157.26.113		194	RADIUS	Access-Request id=0
0.046784000 10.157.26.113	10.157.26.113	204	RADIUS	Access-Challenge id=0
0.000473000 10.157.26.113		290	RADIUS	Access-Request id=1
0.004286000 10.157.26.113	10.157.26.113	84	RADIUS	Access-Reject id=1

Frame 3853: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)

Ethernet II, Src: CiscoMer_fe:f3:56 (98:18:88:fe:f3:56), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)

802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 1010

Internet Protocol Version 4, Src: 10.157.26.113, Dst: [redacted]

User Datagram Protocol, Src Port: 35585, Dst Port: 1812

RADIUS Protocol

Code: Access-Request (1)

Packet Identifier: 0x0 (0)

Length: 148

Authenticator: 77ac6e9af7c3b6112fd5c3b38d193aaf
[The response to this request is in frame 3863]

Attribute Value Pairs

- AVP: t=User-Name(1) 1=19 val=meraki_8021x_test
 - Type: 1
 - Length: 19
 - User-Name: meraki_8021x_test
- AVP: t=NAS-IP-Address(4) 1=6 val=6.254.243.86
- AVP: t=Calling-Station-Id(31) 1=19 val=02-00-00-00-00-01
- AVP: t=Framed-MTU(12) 1=6 val=1400
- AVP: t=NAS-Port-Type(61) 1=6 val=Wireless-802.11(19)
- AVP: t=Service-Type(6) 1=6 val=Framed(2)
- AVP: t=Connect-Info(77) 1=24 val=CONNECT 11Mbps 802.11b
- AVP: t=EAP-Message(79) 1=24 Last Segment[1]

Access Policy Configuration Verification

1. Need to check the parameter mentioned in the access policy is correct and includes Host IP, Port Number, and Secret Key.

Search Dashboard

This network is acting as the configuration template for [231 networks](#).

Access policies

Name: Forescout MAB

Authentication method: my RADIUS server

RADIUS servers

#	Host	Port	Secret	Actions
1	[redacted]	1812	*****	⚙️ ✖️ Test
2	[redacted]	1812	*****	⚙️ ✖️ Test

[Add a server](#)

2. Configured radius server IPs are dummy or not used in production or Access policy is not in use. It is recommended to remove the access policy. If you want to keep it, you can disable the **Radius testing setting**.

Meraki

Small_Site

Network-wide

Security & SD-WAN

Switch

Wireless

Organization

Search Dashboard

Announcer

This network is acting as the configuration template for 231 networks.

Access policies

Name

Forescout MAB

Authentication method

my RADIUS server

RADIUS servers

#	Host	Port	Secret	Actions
1		1812		<div><div></div><div></div></div> <div>Test</div>
2		1812		<div><div></div><div></div></div> <div>Test</div>

Add a server

RADIUS testing

RADIUS testing enabled

RADIUS testing enabled

RADIUS testing disabled

RADIUS CoA support

RADIUS accounting

RADIUS accounting enabled

RADIUS accounting servers

#	Host	Port	Secret	Actions
1		1813		<div><div></div><div></div></div> <div>Test</div>
2		1813		<div><div></div><div></div></div> <div>Test</div>

Add a server

Related Information

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- [Technical Support & Documentation - Cisco Systems](#)

Note

- When the radius servers poll Meraki devices use the LAN IP and Default username “meraki_8021x_test”, the Meraki dashboard used the Meraki MAC address as the source.
- Meraki provided visibility to these alerts since October 2021.