

Meraki 디바이스에서 최근 802.1X 오류 알림 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[문제](#)

[Meraki 디바이스에서 RADIUS 테스트는 무엇입니까?](#)

[구성](#)

[네트워크 다이어그램](#)

[확인 및 문제 해결](#)

[802.1X 구성](#)

[802.1X 구성 확인 테스트](#)

[관련 정보](#)

[메모](#)

소개

이 문서에서는 Meraki 디바이스에서 최근 802.1X 오류 알림을 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 Meraki SDWAN(Software-Defined Wide Area Network) 솔루션 이해
- 기본 액세스 정책 및 RADIUS 인증 이해

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

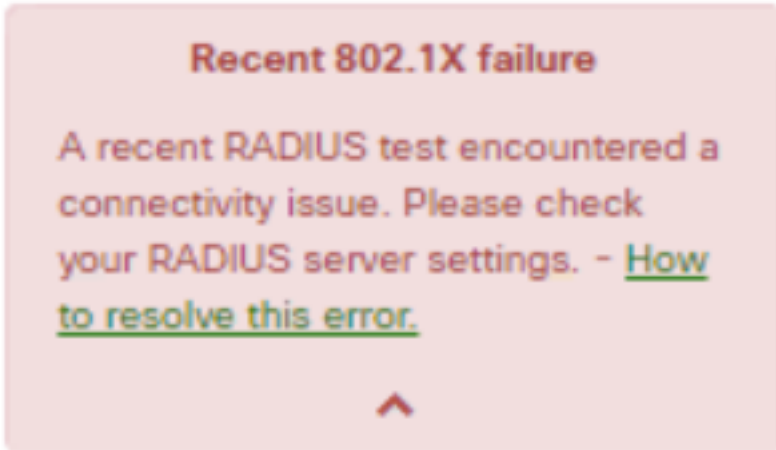
문제

Meraki 디바이스는 AAA radius 서버 정책 컨피그레이션을 사용하여 최종 사용자를 인증합니다.

Meraki 디바이스에서 RADIUS 테스트는 무엇입니까?

최근 802.1X 실패 알림은 구성된 RADIUS 서버로 전송되는 정기 액세스 요청 메시지에 도달할 수 없는 경우 10초의 시간 제한 기간을 사용해야 한다는 것을 표시합니다.

Meraki 디바이스는 RADIUS 서버에 연결할 수 있도록 ID meraki_8021x_test를 사용하는 구성된 RADIUS 서버에 액세스 요청 메시지를 주기적으로 보냅니다. 이러한 Access-Requests의 시간 제한은 10초이며 RADIUS 서버가 응답하지 않을 경우 RADIUS 서버가 연결할 수 없는 것으로 간주하고 "Recent 802.1X failure"(최근 802.1X 실패)" 경고 메시지를 표시합니다. 디바이스에 표시되는 경고의 스크린샷을 참조하십시오.



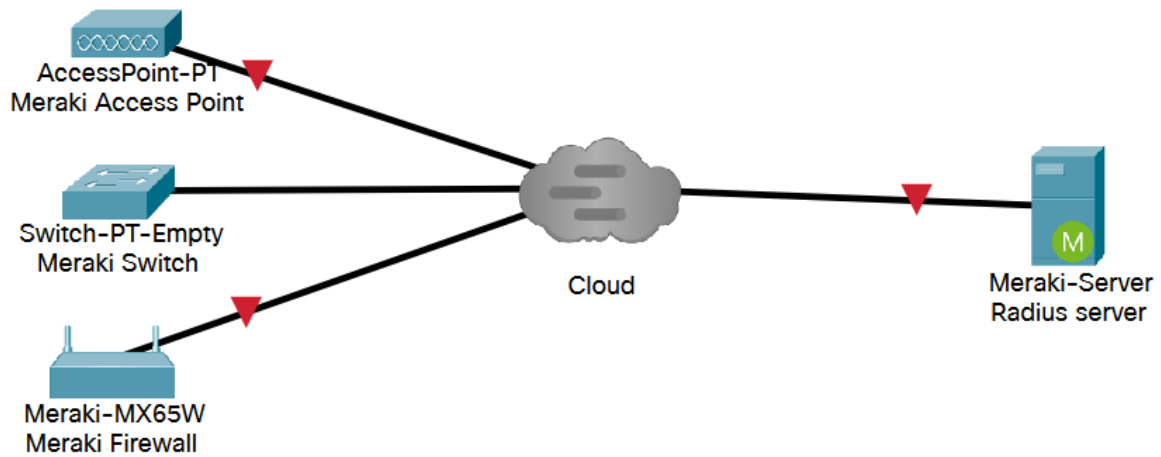
Meraki 디바이스가 서버에서 합법적인 RADIUS 응답(Access-Accept/Reject/Challenge)을 수신하는 경우 테스트가 성공한 것으로 간주됩니다.

RADIUS 테스트가 활성화되면 테스트 결과와 상관없이 모든 RADIUS 서버는 24시간마다 한 번 이상 모든 노드에서 테스트 실행을 유지합니다. 지정된 노드에 대해 RADIUS 테스트가 실패할 경우 통과한 결과가 발생할 때까지 매시간마다 다시 테스트합니다. 후속 단계에서는 서버에 연결할 수 있음을 표시하고, 알림을 지우고, 24시간 테스트 주기로 돌아갑니다.

구성

네트워크 다이어그램

다음은 설정을 설명하는 간단한 토폴로지 다이어그램입니다.



확인 및 문제 해결

802.1X 구성

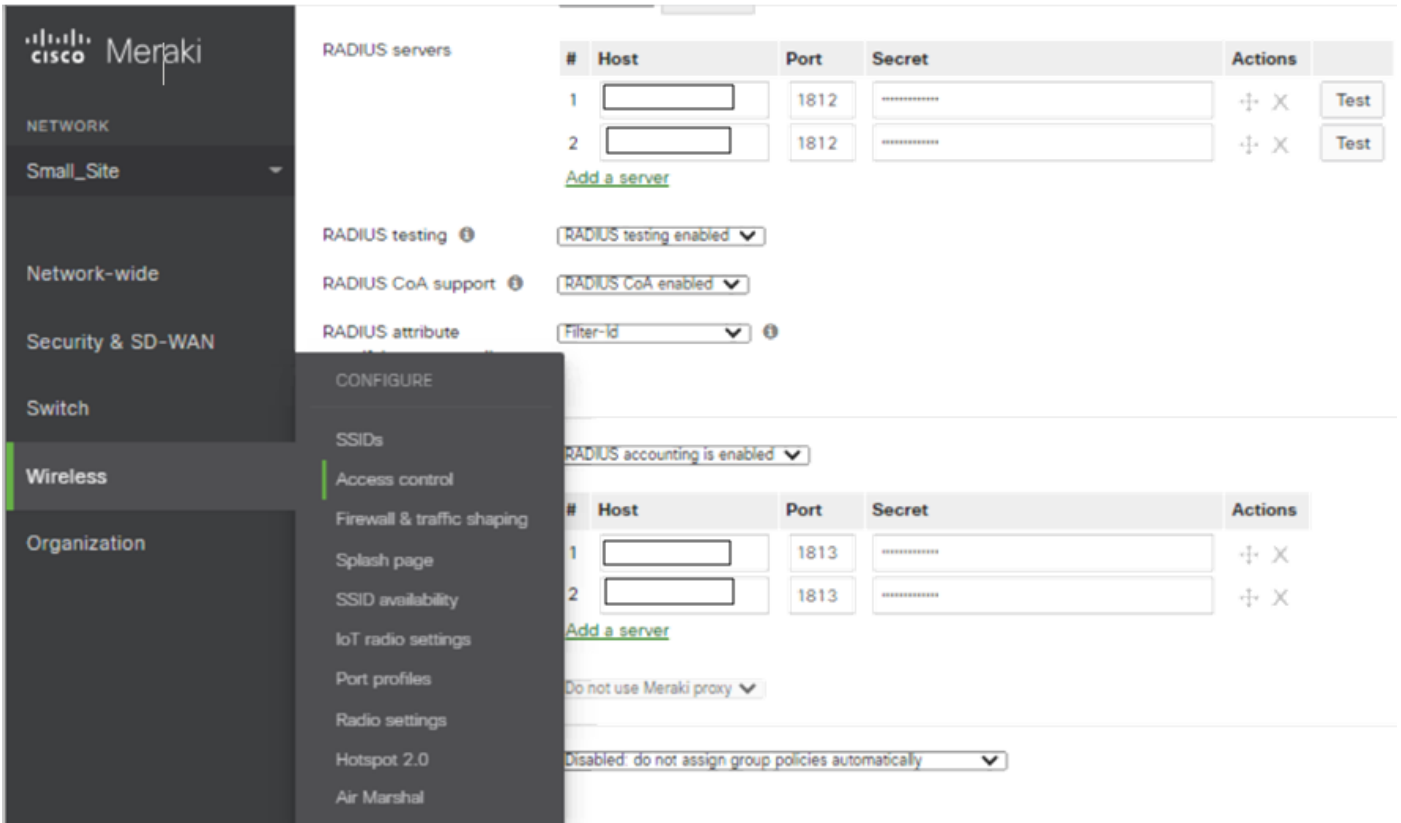
802.1X RADIUS 구성은 Meraki 제품 모델에 따라 표시되는 경로에서 확인할 수 있습니다.

1. MX-Security Appliance(액세스 포트 또는 무선용으로 구성)

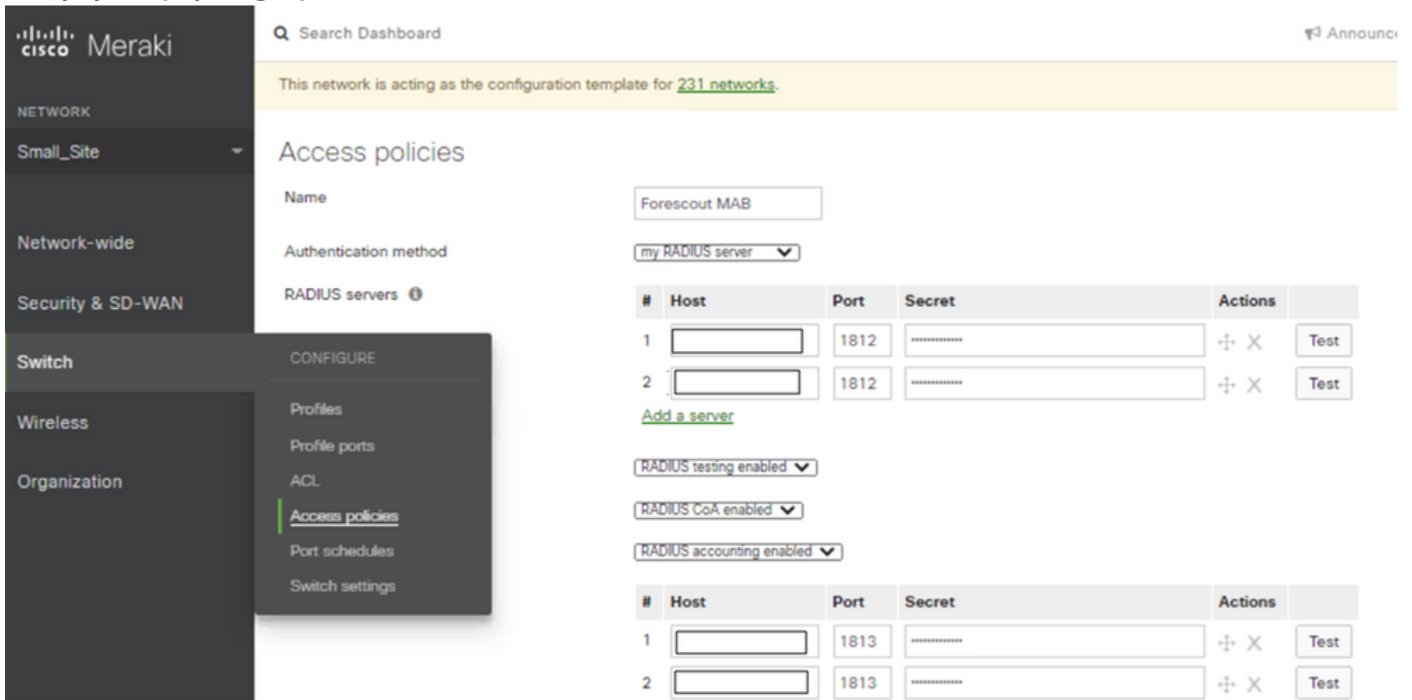
- 액세스 포트의 경우
보안 및 SD-WAN > 주소 지정 및 VLAN

- 무선
보안 및 SD-WAN > 무선 설정

2. MR-Access 포인트(SSID(Service Set Identifier) 단위로 사용): 무선 > 액세스 제어



3. MS-스위치 스위치 > 액세스 정책



802.1X 구성 확인 테스트

- Meraki Dashboard(Meraki 대시보드) > Network Template(네트워크 템플릿) > Switch(스위치) > Access Policies(액세스 정책) > Radius Servers(RADIUS 서버) > 테스트
- Meraki 대시보드 > 네트워크 템플릿 > 무선 > 액세스 제어 > RADIUS 서버 > 테스트

1. 테스트 결과가 모든 AP가 radius 서버에 연결하지 못했음을 나타내면 액세스 요청이 삭제된 위치

를 확인해야 합니다.

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

Total switches: 2
Switches passed: 0
Switches failed: 2
Switches unreachable: 0

2 switches failed to connect to the RADIUS
server.

RADIUS attributes used:

RADIUS attributes unused:

or close

2. 업링크 포트에서 패킷 캡처를 실행하고 액세스 요청 흐름을 확인합니다. 패킷 캡처 액세스의 스크린샷을 참조하십시오. - 요청에 응답이 없습니다.

Time	Source	Destination	Length	Protocol	Info
0.000000000	10.157.229.49	[redacted]	194	RADIUS	Access-Request id=0
1.000321000	10.157.229.49	[redacted]	194	RADIUS	Access-Request id=0, Duplicate Request
2.001830000	10.157.229.49	[redacted]	194	RADIUS	Access-Request id=0, Duplicate Request

3. 확인된 테스트 결과가 accept/reject/deny/response/incorrect credentials로 응답되면 radius 서버가 활성 상태임을 의미합니다.

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:

or [close](#)

4. 업링크 포트에서 패킷 캡처를 실행하고 액세스 요청 흐름을 확인합니다. 패킷 캡처 액세스의 스크린샷을 참조하십시오. 요청에 응답이 있습니다.

Time delta from previous displayed frame	Source	Destination	Length	Protocol	Info
0.000000000	10.157.26.113		194	RADIUS	Access-Request id=0
0.046784000		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	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: 
> 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=02-00-00-00-00-00-01
      > 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]
  
```

액세스 정책 컨피그레이션 확인

1. 액세스 정책에 언급된 매개변수가 올바른지 확인하고 호스트 IP, 포트 번호 및 비밀 키를 포함해야 합니다.

The screenshot shows the Cisco Meraki dashboard interface. On the left is a navigation sidebar with categories like NETWORK, Small_Site, Network-wide, Security & SD-WAN, Switch, and Wireless. The main content area displays 'Access policies' for a policy named 'Forescout MAB'. The configuration includes:

- Name:** Forescout MAB
- Authentication method:** my RADIUS server
- RADIUS servers:** A table with 2 entries:

#	Host	Port	Secret	Actions
1	<input type="text"/>	1812	<input type="password"/>	⬇️ ✖️ Test
2	<input type="text"/>	1812	<input type="password"/>	⬇️ ✖️ Test

At the bottom of the RADIUS servers table, there is a link 'Add a server'.

2. 구성된 Radius 서버 IP가 더미 또는 프로덕션 환경에서 사용되지 않거나 액세스 정책이 사용 중이 아닙니다. 액세스 정책을 제거하는 것이 좋습니다. 유지하려는 경우 Radius 테스트 설정을 비활성화할 수 있습니다.

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	<input type="text"/>	1812	⊕ × Test
2	<input type="text"/>	1812	⊕ × Test

[Add a server](#)

RADIUS testing: RADIUS testing enabled

RADIUS CoA support

RADIUS accounting: RADIUS accounting enabled

RADIUS accounting servers

#	Host	Port	Secret	Actions
1	<input type="text"/>	1813	⊕ × Test
2	<input type="text"/>	1813	⊕ × Test

[Add a server](#)

관련 정보

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- [기술 지원 및 문서 - Cisco Systems](#)

메모

- radius 서버가 Meraki 디바이스를 폴링할 때 LAN IP 및 기본 사용자 이름 "meraki_8021x_test"를 사용할 때 Meraki 대시보드는 Meraki MAC 주소를 소스로 사용했습니다.
- Meraki는 2021년 10월부터 이러한 경고에 대한 가시성을 제공했습니다.