

Probleemoplossing recente melding 802.1X fout in Meraki-apparaat

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Wat is de RADIUS-test in Meraki-apparaten?](#)

[Configureren](#)

[Netwerkdigram](#)

[Probleemoplossing controleren](#)

[802.1x-configuratie](#)

[802.1X controletest voor de configuratie](#)

[Gerelateerde informatie](#)

[Opmerking](#)

Inleiding

In dit document wordt beschreven hoe de recente melding van 802.1X-fouten in het Meraki-apparaat moet worden opgelost.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Begrijp de basisoplossing van Meraki voor softwaregedefinieerde Wide Area Network (SDWAN)
- Basistoegangsbeleid en radiofrequentie-verificatie begrijpen

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de

mogelijke impact van om het even welke opdracht begrijpt.

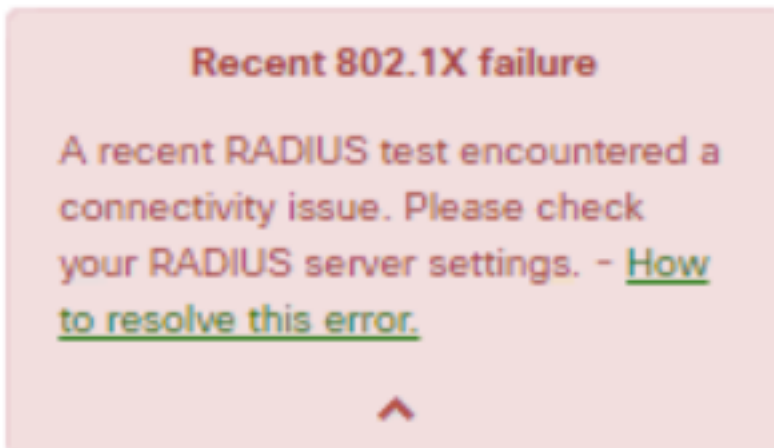
Probleem

Meraki-apparaten gebruiken de AAA-serverbeleidsconfiguratie om de eindgebruiker voor het eerst te authentifieren.

Wat is de RADIUS-test in Meraki-apparaten?

De recente melding van 802.1X is weergegeven. Als de periodieke berichten met een toegangsaanvraag die naar de geconfigureerde RADIUS-servers zijn verzonden, onbereikbaar zijn, moet u een tijdelijke periode van 10 seconden gebruiken.

Meraki-apparaten sturen regelmatig berichten met een toegangsaanvraag naar de geconfigureerde RADIUS-servers die een identiteit **meraki_8021x_test** gebruiken om er zeker van te zijn dat de RADIUS-servers bereikbaar zijn. Deze toegangsaanvragen hebben een onderbreking van 10 seconden en als de RADIUS-server niet reageert, worden de Straalservers onbereikbaar geacht en wordt de waarschuwing "Recent 802.1X fail" bericht gevraagd. Raadpleeg de screenshot van de waarschuwing op het apparaat:



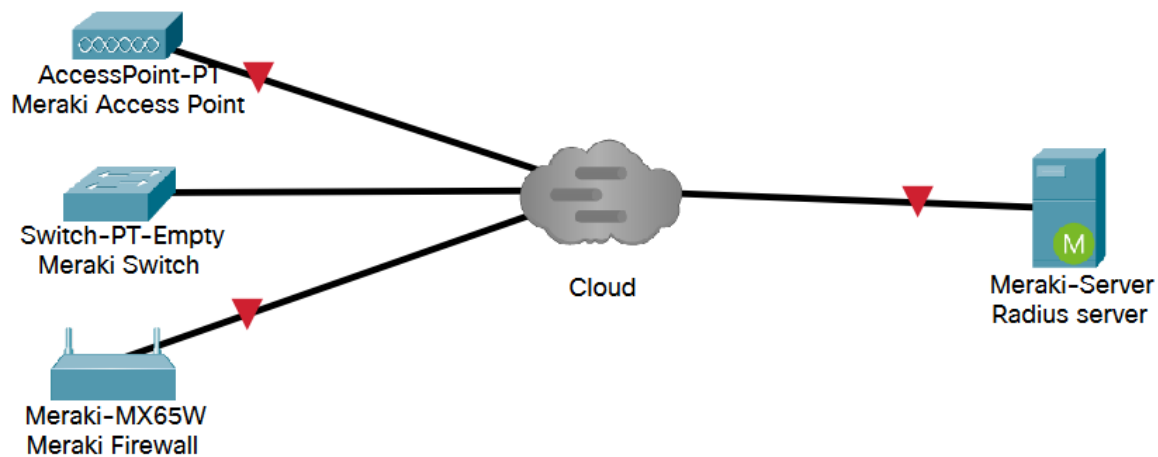
Een test wordt als succesvol beschouwd als het Meraki-apparaat een legitieme RADIUS-respons (Access-Accept/Afwerp/Challenge) van de server ontvangt.

Als de RADIUS-test is ingeschakeld, worden alle RADIUS-servers minstens één keer per 24 uur op elk knooppunt uitgevoerd, ongeacht het testresultaat. Als een RADIUS-test voor een bepaald knooppunt mislukt, wordt elk uur opnieuw getest tot een resultaat dat doorgaat. Een volgende pas tekent de server bereikbaar, ontruimt de waakzaamheid en keert terug naar de testcyclus van 24 uur.

Configureren

Netwerkdigram

Hier is een eenvoudig topologiedigram dat de instellingen beschrijft:



Probleemoplossing controleren

802.1x-configuratie

De configuratie van 802.1X RADIUS kan worden gevonden in het afgebeelde pad dat afhankelijk is van het Meraki-productmodel.

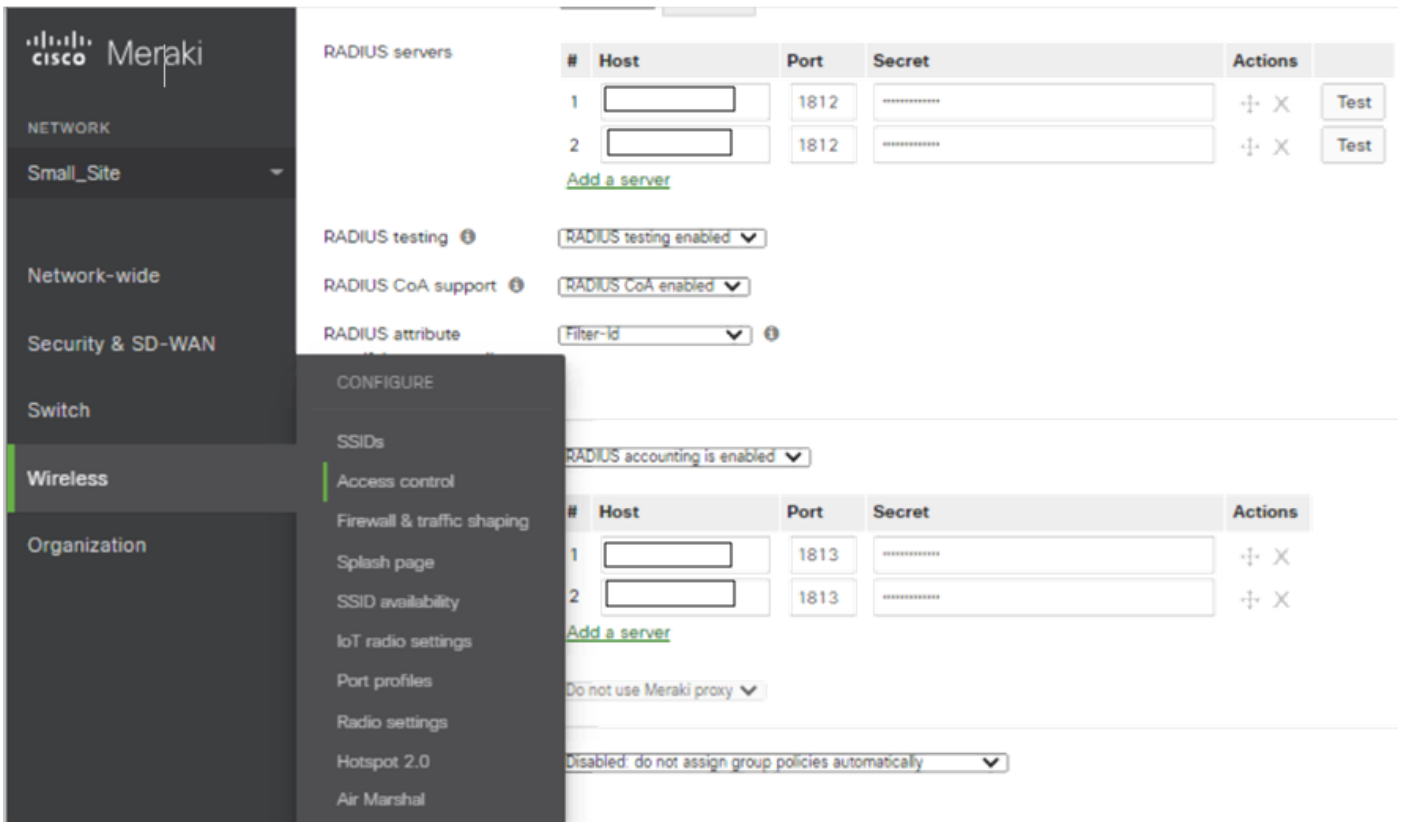
1. MGX-security applicatie (geconfigureerd voor ofwel toegangsporten ofwel draadloos)

- Voor toegangsporten
Security en SD-WAN > adressering en VLAN's

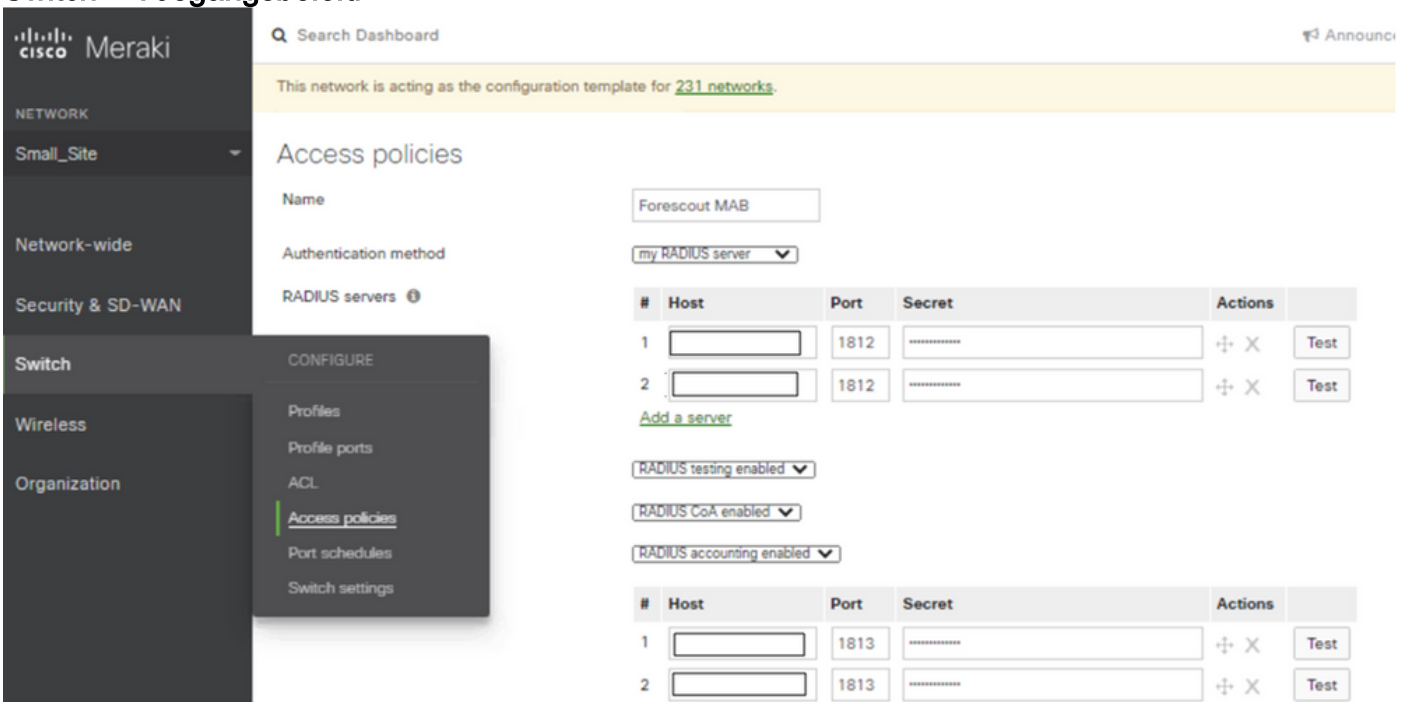
- Voor draadloos
Beveiliging en SD-WAN > Draadloze instellingen

The screenshot shows the Meraki dashboard interface. The left sidebar contains navigation options: NETWORK, Network-wide, Cellular Gateway, Security & SD-WAN (highlighted), Switch, Wireless, and Organization. The main content area displays the 'Access control' configuration for 'LAN (1)'. Under the 'CONFIGURE' section, the 'Access control' option is selected, showing three radio button options: 'None (direct access)' (selected), 'Click-through', and 'Sign-on with my RADIUS server'. A search bar and a notification banner are visible at the top of the dashboard.

2. MR-access points (ingeschakeld op basis van een SSID (Service Set Identifier)):
Draadloos > toegangscontrole



3. MS-Switches Switch > Toegangsbeleid



802.1X controletest voor de configuratie

- Meraki dashboard > Netwerksjabloon > Switch > Toegangsbeleid > RADIUS-servers > Test
- Meraki Dashboard > Netwerksjabloon > Draadloos > Toegangsbeheer > Straalservers > Test

1. Als het testresultaat wordt opgemerkt aangezien **Alle AP er niet in slaagde om de radiogateway aan te sluiten**, moet u controleren waar het toegangs-verzoek is gevallen.

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

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

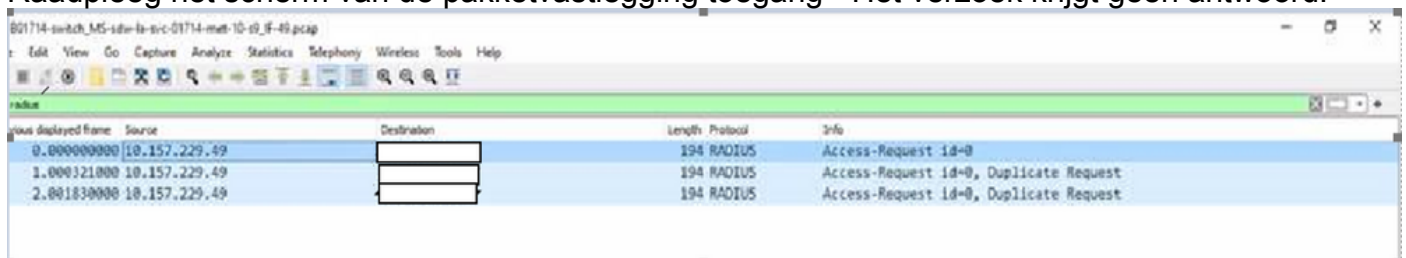
2 switches failed to connect to the RADIUS
server.

RADIUS attributes used:

RADIUS attributes unused:

or close

2. Start de pakketvastlegging op de uplinks-poort en controleer de toegangsaanvraag-stroom. Raadpleeg het scherm van de pakketvastlegging toegang - Het verzoek krijgt geen antwoord.



The screenshot shows a Wireshark capture of RADIUS traffic. The interface includes a menu bar (Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The main display area shows a list of captured packets with the following columns: 'Time Displayed Frame', 'Source', 'Destination', 'Length', 'Protocol', and 'Info'. Three RADIUS packets are visible, all originating from 10.157.229.49. The first packet is an 'Access-Request id=0'. The second and third packets are 'Duplicate Request'.

Time Displayed Frame	Source	Destination	Length	Protocol	Info
0.000000000	10.157.229.49	[redacted]	194	RADIUS	Access-Request id=0
1.000321800	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. Als het opvallende testresultaat wordt beantwoord als aanvaarden/afwijzen/antwoorden/onjuiste geloofsbrieven, betekent dit dat de straal server leeft.

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. Start de pakketvastlegging op de uplinks-poort en controleer de toegangsaanvraag-stroom. Raadpleeg het screenshot van de pakketvastlegging toegang - het verzoek kreeg een antwoord.

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

Verificatie van toegangsbeleid

1. De noodzaak om de in het toegangsbeleid vermelde parameter te controleren is correct en omvat Host IP, Port Number en Secret Key.

Search Dashboard Announ

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

Access policies

Name:

Authentication method:

RADIUS servers ?

#	Host	Port	Secret	Actions
1	<input type="text"/>	1812	<input type="text"/>	⊕ × Test
2	<input type="text"/>	1812	<input type="text"/>	⊕ × Test

[Add a server](#)

2. De IP's die zijn geconfigureerd, zijn dummy of worden niet gebruikt in het productiebeleid of het toegangsbeleid is niet in gebruik. Aanbevolen wordt het toegangsbeleid te schrappen. Als u dit wilt behouden, kunt u de **instelling** voor het **testen van straal** uitschakelen.

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](#)

Gerelateerde informatie

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- [Technische ondersteuning en documentatie – Cisco Systems](#)

Opmerking

- Wanneer de sleuven Meraki-apparaten hebben gevraagd om de LAN IP- en standaardgebruikersnaam voor "meraki_8021x_test", werd het Meraki-dashboard als bron gebruikt.
- Meraki heeft deze waarschuwingen sinds oktober 2021 zichtbaar gemaakt.