

# Dépannage des alertes de défaillance 802.1X récentes sur le périphérique Meraki

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Problème](#)

[Quel est le test RADIUS dans les appareils Meraki ?](#)

[Configuration](#)

[Diagramme du réseau](#)

[Vérifiez et dépannez](#)

[Configuration 802.1X](#)

[Test de vérification de configuration 802.1X](#)

[Informations connexes](#)

[Remarque](#)

## Introduction

Ce document décrit comment résoudre la récente alerte de défaillance 802.1X dans le périphérique Meraki.

## Conditions préalables

### Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comprendre la solution de base SDWAN (Wide Area Network) définie par logiciel Meraki
- Comprendre la stratégie d'accès de base et l'authentification Radius

### Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

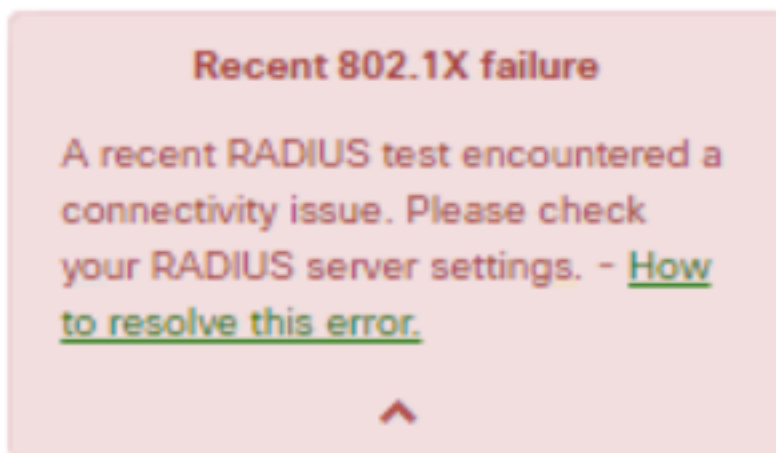
# Problème

Les périphériques Meraki utilisent la configuration de la stratégie de serveur AAA radius pour authentifier l'utilisateur final.

## Quel est le test RADIUS dans les appareils Meraki ?

L'alerte d'échec 802.1X récente indique que si les messages de demande d'accès périodiques envoyés aux serveurs RADIUS configurés sont inaccessibles, vous devez utiliser un délai d'expiration de 10 secondes.

Les périphériques Meraki envoient régulièrement des messages de demande d'accès aux serveurs RADIUS configurés qui utilisent l'identité **meraki\_8021x\_test** pour s'assurer que les serveurs RADIUS sont accessibles. Ces demandes d'accès ont un délai d'attente de 10 secondes et si le serveur RADIUS ne répond pas, il considère que les serveurs RADIUS sont inaccessibles et invite le message d'alerte « Récent échec 802.1X ». Reportez-vous à la capture d'écran de l'alerte affichée sur le périphérique :



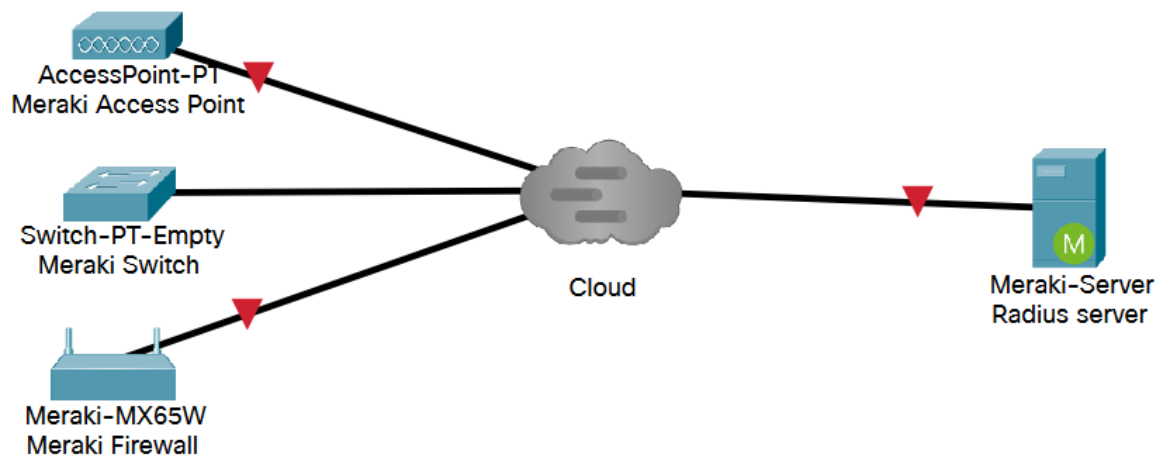
Un test est considéré comme réussi si le périphérique Meraki reçoit une réponse RADIUS légitime (Access-Accept/Reject/Challenge) du serveur.

Lorsque le test RADIUS est activé, tous les serveurs RADIUS sont maintenus en série sur chaque noeud au moins une fois par 24 heures, quel que soit le résultat du test. Si un test RADIUS échoue pour un noeud donné, il teste à nouveau toutes les heures jusqu'à ce qu'un résultat qui passe se produise. Une passe ultérieure marque le serveur accessible, efface l'alerte et revient au cycle de test de 24 heures.

## Configuration

### Diagramme du réseau

Voici un schéma de topologie simple qui décrit la configuration :



## Vérifiez et dépannez

### Configuration 802.1X

La configuration RADIUS 802.1X se trouve dans le chemin indiqué qui dépend du modèle de produit Meraki.

#### 1. Dispositif de sécurité MX (configuré pour les ports d'accès ou sans fil)

- Pour les ports d'accès  
**Sécurité et SD-WAN > Adressage et VLAN**
- Pour les réseaux sans fil  
**Sécurité et SD-WAN > Paramètres sans fil**

Search Dashboard

Announcements

This network is acting as the configuration template for [2 networks](#).

Access control

Select VLAN: **LAN (1)**

CONFIGURE

- Addressing & VLANs
- Wireless settings
- DHCP
- Firewall
- Site-to-site VPN
- Client VPN
- Active Directory
- SD-WAN & traffic shaping
- Threat protection
- Content filtering
- Access control**
- Splash page

None (direct access)  
Users can access the network as soon as they associate

Click-through  
Users must view and acknowledge your splash page before being allowed on the network

Sign-on with **my RADIUS server**

Last login: 12 minutes ago from your current IP address  
Current session started: 12 minutes ago  
Data for WELLS FARGO UTILITY NET (organization ID: 480998) is hosted in North America

#### 2. Points d'accès MR (activés par SSID (Service Set Identifier)) : **Sans fil > Contrôle d'accès**

**RADIUS servers**

#	Host	Port	Secret	Actions
1	<input type="text"/>	1812	.....	↕ X Test
2	<input type="text"/>	1812	.....	↕ X Test

[Add a server](#)

RADIUS testing:

RADIUS CoA support:

RADIUS attribute:

RADIUS accounting is enabled:

### 3. Commutateurs MS

#### Commutateur > Politiques d'accès

**Access policies**

Name:

Authentication method:

RADIUS servers:

#	Host	Port	Secret	Actions
1	<input type="text"/>	1812	.....	↕ X Test
2	<input type="text"/>	1812	.....	↕ X Test

[Add a server](#)

RADIUS testing enabled:

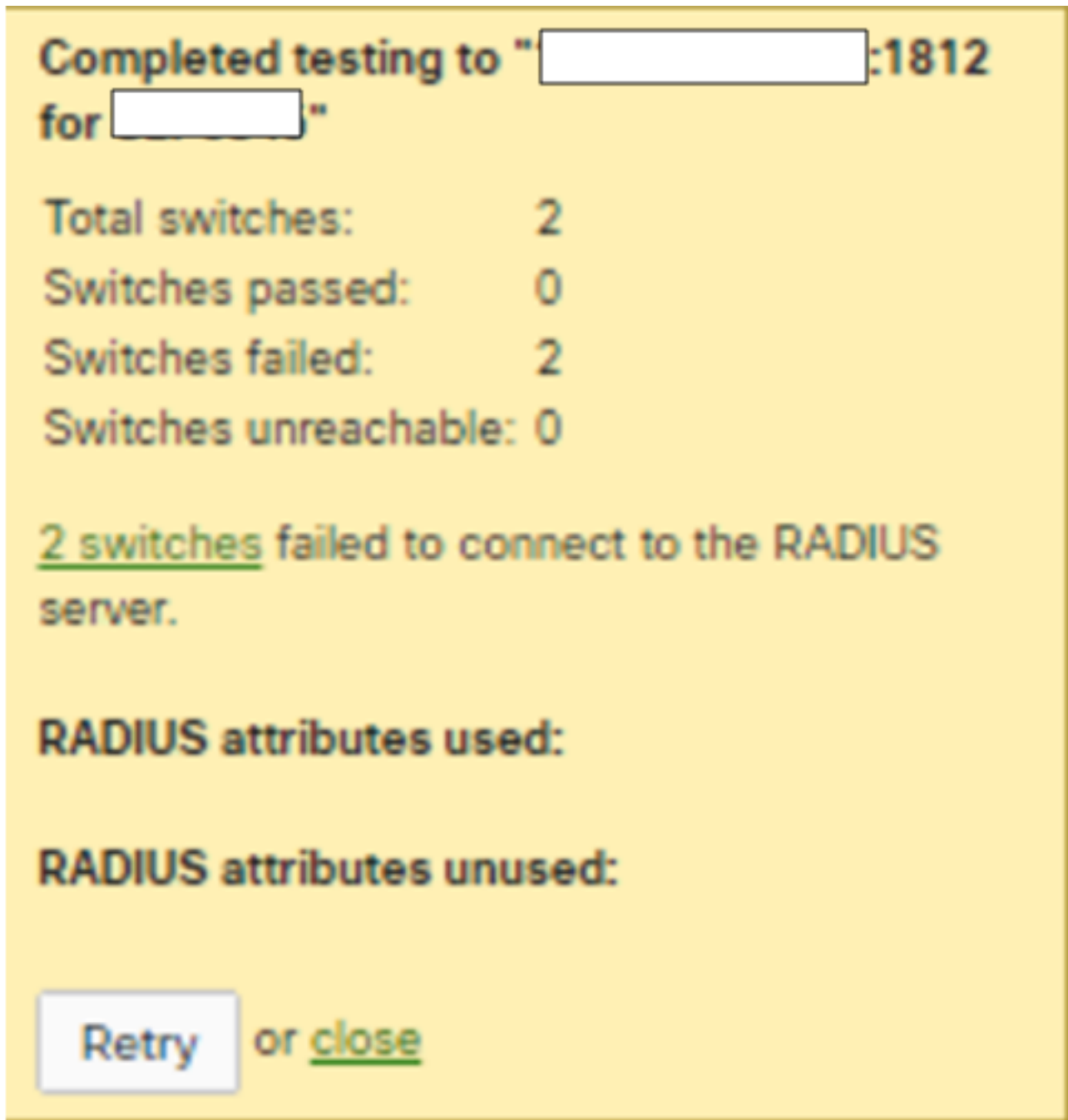
RADIUS CoA enabled:

RADIUS accounting enabled:

#### Test de vérification de configuration 802.1X

- Tableau de bord Meraki > Modèle de réseau > Commutateur > Stratégies d'accès > Serveurs Radius > Tester
- Tableau de bord Meraki > Modèle de réseau > Accès sans fil > Contrôle d'accès > Serveurs Radius > Tester

1. Si le résultat du test est remarqué alors que **All AP n'a pas réussi à connecter le serveur radius**, vous devez vérifier où la demande d'accès a été abandonnée.



2. Exécutez la capture de paquets sur le port de liaison ascendante et vérifiez le flux de demande d'accès. Reportez-vous à la capture d'écran de l'accès à la capture de paquets : la requête n'obtient aucune réponse.

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. Si le résultat de test remarqué reçoit une réponse en tant qu'informations d'identification d'acceptation/rejet/refus/réponse/incorrectes, cela signifie que le serveur radius est actif.

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. Exécutez la capture de paquets sur le port de liaison ascendante et vérifiez le flux de demande d'accès. Reportez-vous à la capture d'écran de l'accès à la capture de paquets - La demande a reçu une réponse.

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]
  
```

## Vérification de la configuration de la stratégie d'accès

1. Vous devez vérifier que le paramètre mentionné dans la stratégie d'accès est correct et inclut l'adresse IP de l'hôte, le numéro de port et la clé secrète.

Search Dashboard Announ

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	.....	⊕ × Test
2		1812	.....	⊕ × Test

[Add a server](#)

2. Les adresses IP de serveur RADIUS configurées sont factices ou ne sont pas utilisées dans la production ou la stratégie d'accès n'est pas utilisée. Il est recommandé de supprimer la stratégie d'accès. Si vous voulez le conserver, vous pouvez désactiver le **paramètre de test RADIUS**.

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 testing disabled

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](#)

## Informations connexes

- [https://documentation.meraki.com/General\\_Administration/Cross-Platform\\_Content/Alert\\_-\\_Recent\\_802.1X\\_Failure](https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure)
- [Support et documentation techniques - Cisco Systems](#)

## Remarque

- Lorsque les serveurs radius interrogent les périphériques Meraki à l'aide de l'adresse IP LAN et du nom d'utilisateur par défaut "meraki\_8021x\_test", le tableau de bord Meraki utilise l'adresse MAC Meraki comme source.
- Meraki a fourni une visibilité sur ces alertes depuis octobre 2021.