

對Meraki裝置中的最近802.1X故障警報進行故障排除

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[問題](#)

[Meraki裝置中的RADIUS測試是什麼？](#)

[設定](#)

[網路圖表](#)

[驗證和疑難排解](#)

[802.1X配置](#)

[802.1X配置驗證測試](#)

[相關資訊](#)

[附註](#)

簡介

本文檔介紹如何解決Meraki裝置中最近的802.1X故障警報。

必要條件

需求

思科建議您瞭解以下主題：

- 瞭解基本的Meraki軟體定義的廣域網(SDWAN)解決方案
- 瞭解基本訪問策略和Radius身份驗證

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

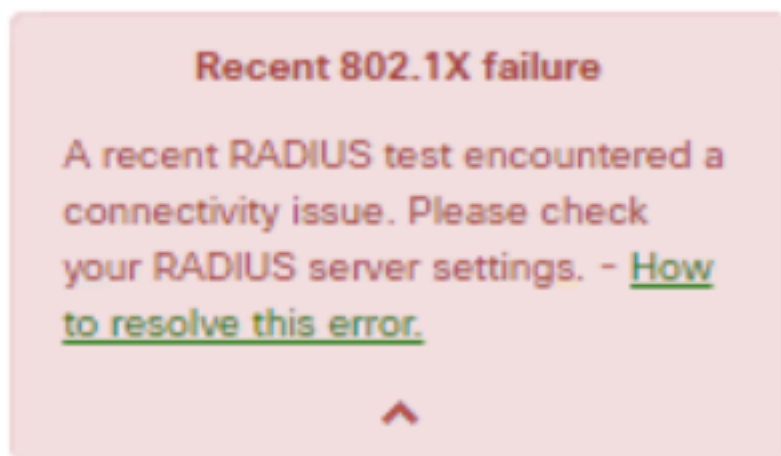
問題

Meraki裝置使用AAA radius伺服器策略配置對終端使用者進行身份驗證。

Meraki裝置中的RADIUS測試是什麼？

最近的802.1X故障警報顯示，如果傳送到配置的RADIUS伺服器的定期訪問請求消息無法訪問，則必須使用10秒的超時時間。

Meraki裝置定期將訪問請求消息傳送到已配置的RADIUS伺服器，這些伺服器使用身份 **meraki_8021x_test** 確保RADIUS伺服器可訪問。這些存取要求逾時10秒，如果RADIUS伺服器沒有回應，便會認為radius伺服器無法連線，並提示警示「Recent 802.1X failure」訊息。請參閱裝置上顯示的警報的螢幕截圖：



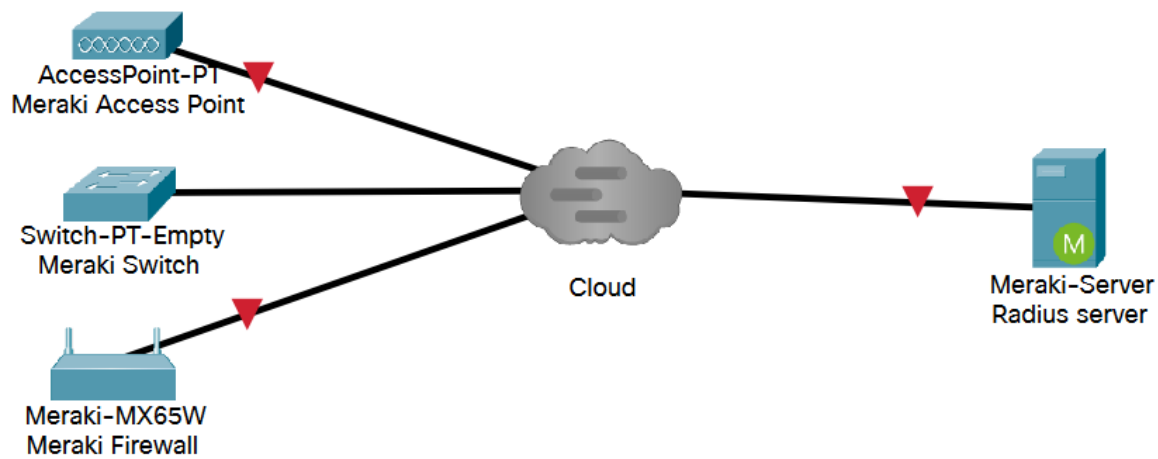
如果Meraki裝置從伺服器收到任何合法RADIUS響應(Access-Accept/Reject/Challenge)，則測試被視為成功。

啟用RADIUS測試後，所有RADIUS伺服器都會在每個節點上保持至少每24小時運行一次的測試，無論測試結果如何。如果對指定節點的RADIUS測試失敗，它每小時重新測試一次，直到出現通過結果。後續的傳遞將標籤伺服器可訪問、清除警報並返回24小時測試週期。

設定

網路圖表

以下是說明此設定的簡單拓撲圖：



驗證和疑難排解

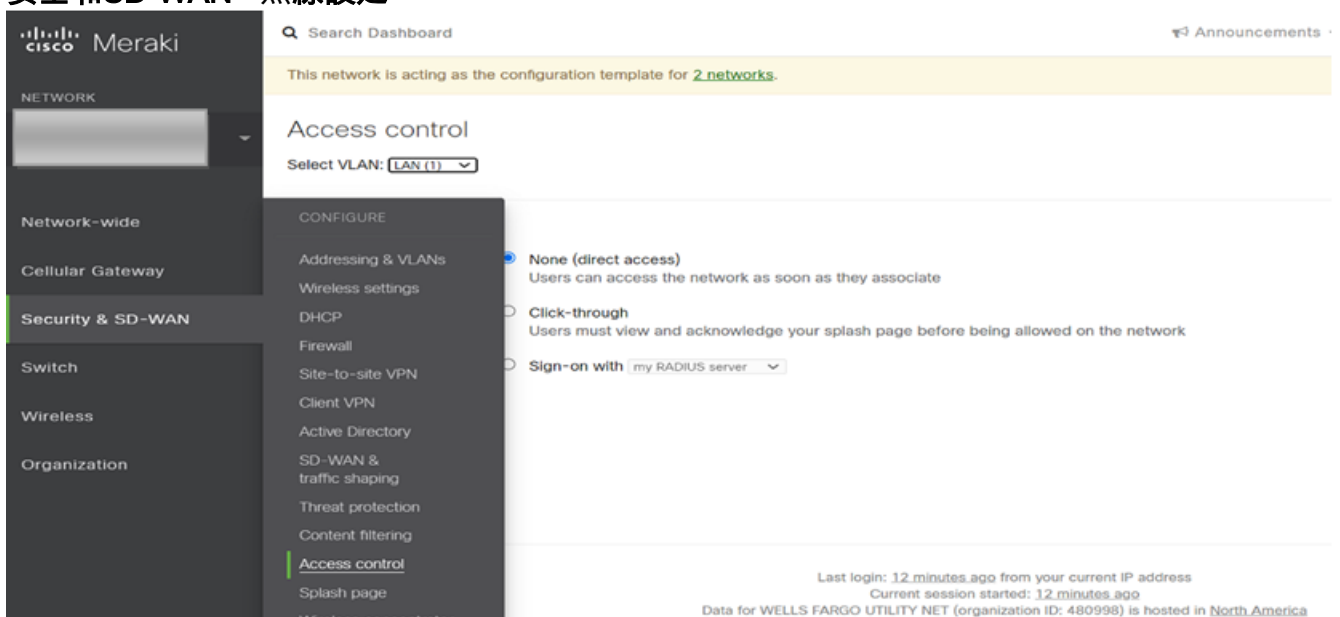
802.1X配置

在顯示的路徑中可找到802.1X RADIUS配置，該路徑取決於Meraki產品型號。

1. MX-Security裝置（針對接入埠或無線配置）

- 對於接入埠
安全與SD-WAN > 編址與VLAN

- 無線
安全和SD-WAN > 無線設定



2. MR-Access points(基於每個服務集識別符號(SSID)啟用): 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 testing enabled**

RADIUS CoA support **RADIUS CoA enabled**

RADIUS attribute **Filter-Id**

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 > 訪問策略

Meraki

NETWORK

Small_Site

Network-wide

Security & SD-WAN

Switch

Wireless

Organization

CONFIGURE

Profiles

Profile ports

ACL

Access policies

Port schedules

Switch settings

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](#)

RADIUS testing enabled

RADIUS CoA enabled

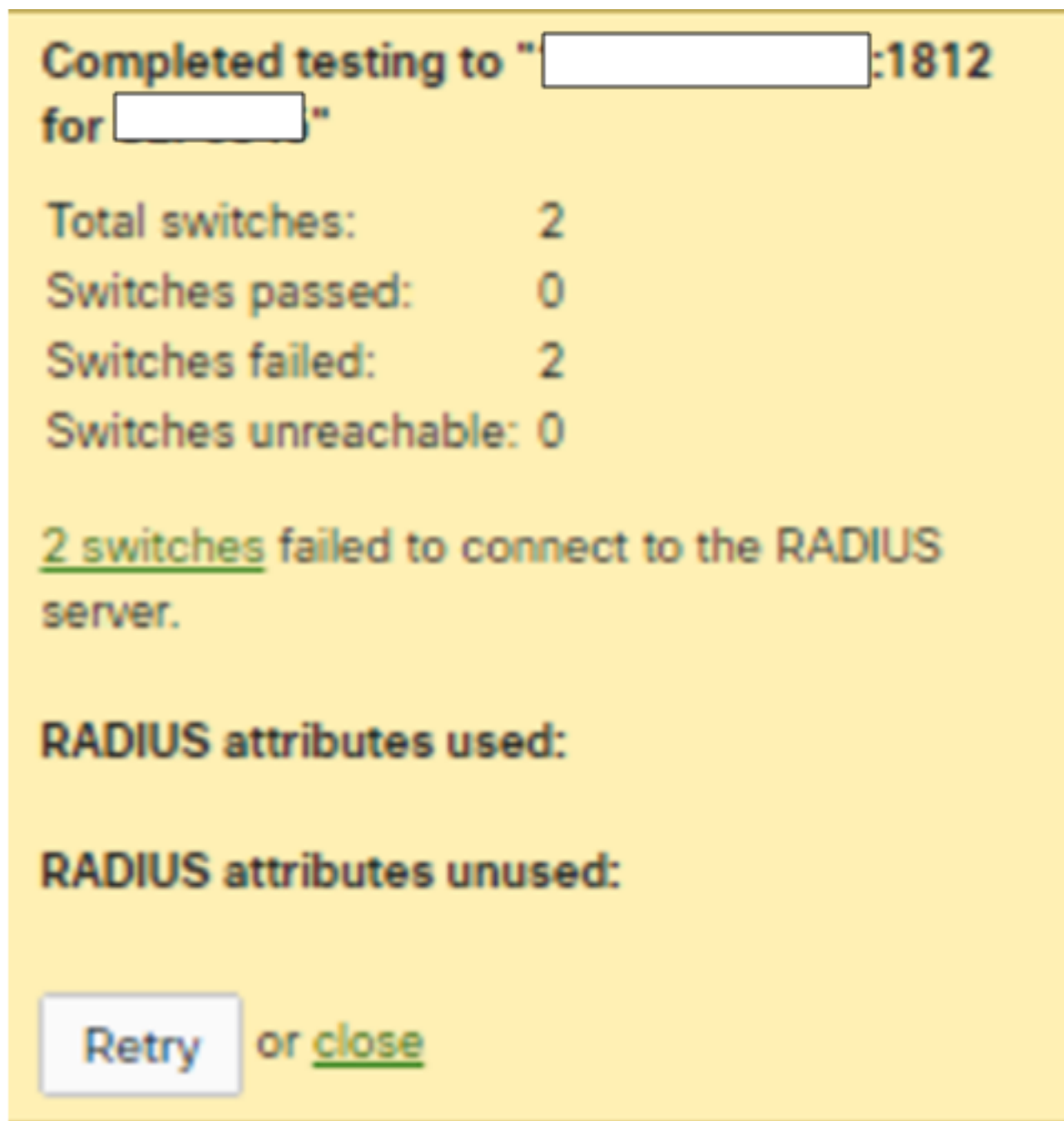
RADIUS accounting enabled

#	Host	Port	Secret	Actions
1		1813	*****	⌵ × Test
2		1813	*****	⌵ × Test

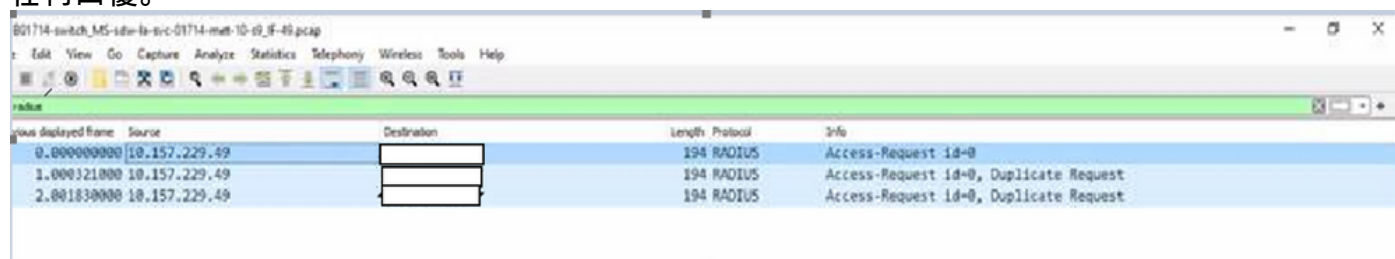
802.1X配置驗證測試

- Meraki控制板 > Network Template > Switch > Access Policies > Radius Servers > 測試
- Meraki控制面板 > 網路模板 > 無線 > 存取控制 > Radius伺服器 > 測試

1.如果測試結果發現所有AP都未能連線radius伺服器，則需要檢查丟棄訪問請求的位置。



2. 在上行鏈路埠上運行資料包捕獲並驗證訪問請求流。請參閱封包擷取存取的截圖 — 要求沒有收到任何回覆。



3. 如果發現測試結果被回覆為接受/拒絕/拒絕/響應/不正確的憑證，則表示radius伺服器處於活動狀態。

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. 在上行鏈路埠上運行資料包捕獲並驗證訪問請求流。請參閱封包擷取存取的截圖 — 要求獲得回覆。

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=02-00-00-00-00-01
>	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]

存取原則組態驗證

1.需要檢查訪問策略中提到的引數是否正確，包括主機IP、埠號和金鑰。

Meraki

NETWORK

Small_Site

Network-wide

Security & SD-WAN

Switch

Wireless

Search Dashboard

Announ

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

Access policies

Name: Forescout MAB

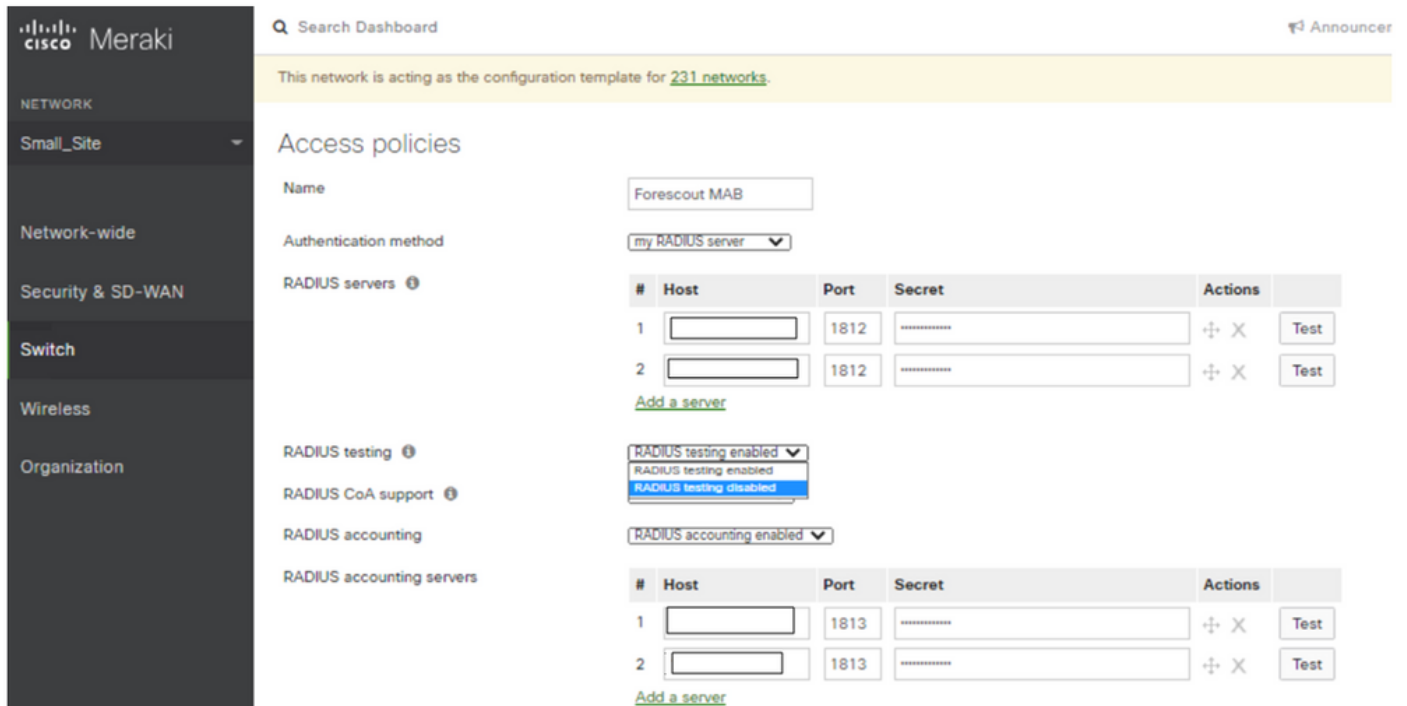
Authentication method: my RADIUS server

RADIUS servers

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

[Add a server](#)

2.配置的RADIUS伺服器IP是虛設的，或未在生產中使用，或者未使用訪問策略。建議刪除訪問策略。如果要保留它，可以禁用Radius測試設定。



相關資訊

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- 技術支援與文件 - Cisco Systems

附註

- 當radius伺服器輪詢Meraki裝置使用LAN IP和預設使用者名稱「meraki_8021x_test」時，Meraki控制面板使用Meraki MAC地址作為源。
- 自2021年10月起，Meraki就提供了這些警報的可視性。