Fehlerbehebung bei kürzlich zurückliegender 802.1X-Fehlermeldung im Meraki-Gerät

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die aktuelle 802.1X-Fehlermeldung im Meraki-Gerät behoben wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundlegende Meraki Software-Defined Wide Area Network (SDWAN)-Lösung
- Grundlegende Zugriffsrichtlinien und Radius-Authentifizierung

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

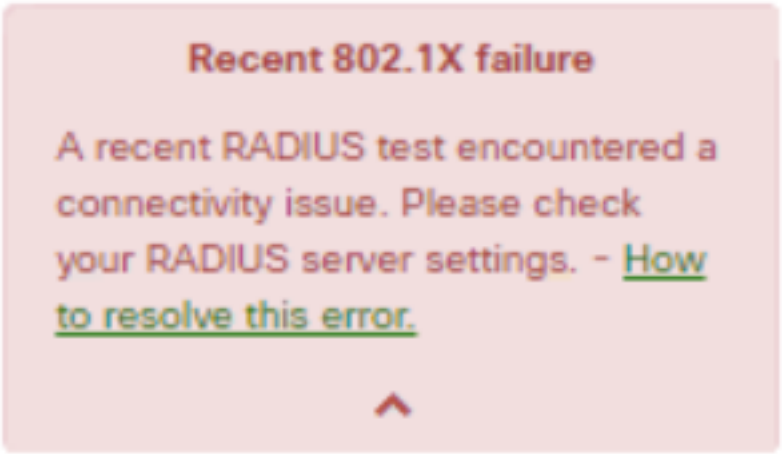
Problem

Meraki-Geräte verwenden die Konfiguration der AAA-Radius-Serverrichtlinien, um den Endbenutzer zu authentifizieren.

Was ist der RADIUS-Test auf Meraki-Geräten?

Die kürzlich angezeigte 802.1X-Fehlerwarnung zeigt an, dass Sie eine Zeitüberschreitung von 10 Sekunden verwenden müssen, wenn die Meldungen für regelmäßige Zugriffsanfragen, die an die konfigurierten RADIUS-Server gesendet werden, nicht erreichbar sind.

Meraki-Geräte senden regelmäßig Access-Request-Nachrichten an die konfigurierten RADIUS-Server, die die Identität **meraki_8021x_test** verwenden, um sicherzustellen, dass die RADIUS-Server erreichbar sind. Diese Zugriffsanfragen haben eine Zeitüberschreitung von 10 Sekunden. Wenn der RADIUS-Server nicht antwortet, werden RADIUS-Server als nicht erreichbar eingestuft und die Warnmeldung "Recent 802.1X failure" (Kürzlicher 802.1X-Fehler) angezeigt. Siehe Screenshot der Warnung auf dem Gerät:



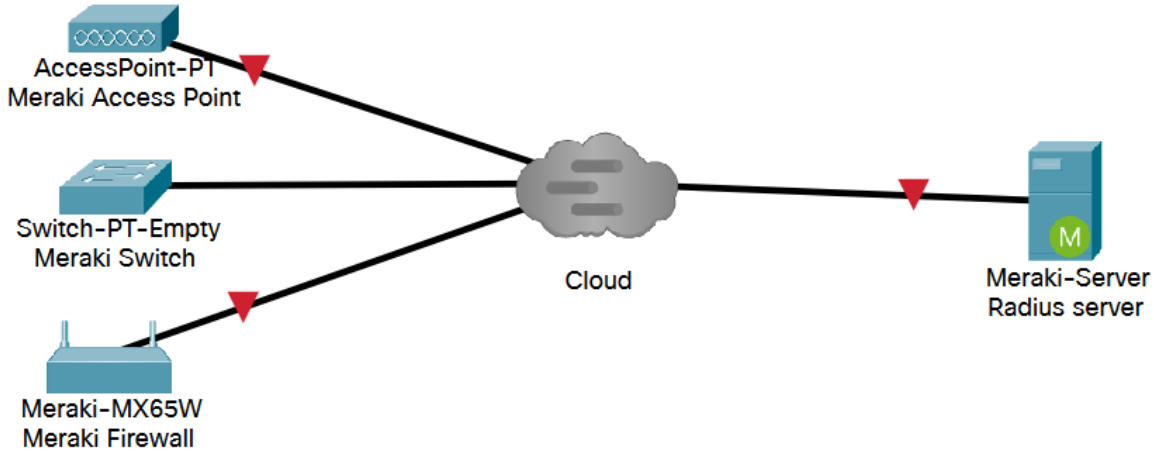
Ein Test wird als erfolgreich angesehen, wenn das Meraki-Gerät vom Server eine legitime RADIUS-Antwort (Access-Accept/Reject/Challenge) erhält.

Wenn der RADIUS-Test aktiviert ist, werden alle RADIUS-Server unabhängig vom Testergebnis mindestens einmal pro 24 Stunden auf jedem Knoten getestet. Wenn ein RADIUS-Test für einen bestimmten Knoten fehlschlägt, wird er stündlich erneut getestet, bis ein Ergebnis vorliegt, das erfolgreich war. Bei einem folgenden Durchlauf wird der Server erreichbar, die Warnmeldung wird gelöscht und der 24-Stunden-Testzyklus wieder aufgenommen.

Konfigurieren

Netzwerkdiagramm

Das folgende einfache Topologiediagramm beschreibt die Konfiguration:



Überprüfung und Fehlerbehebung

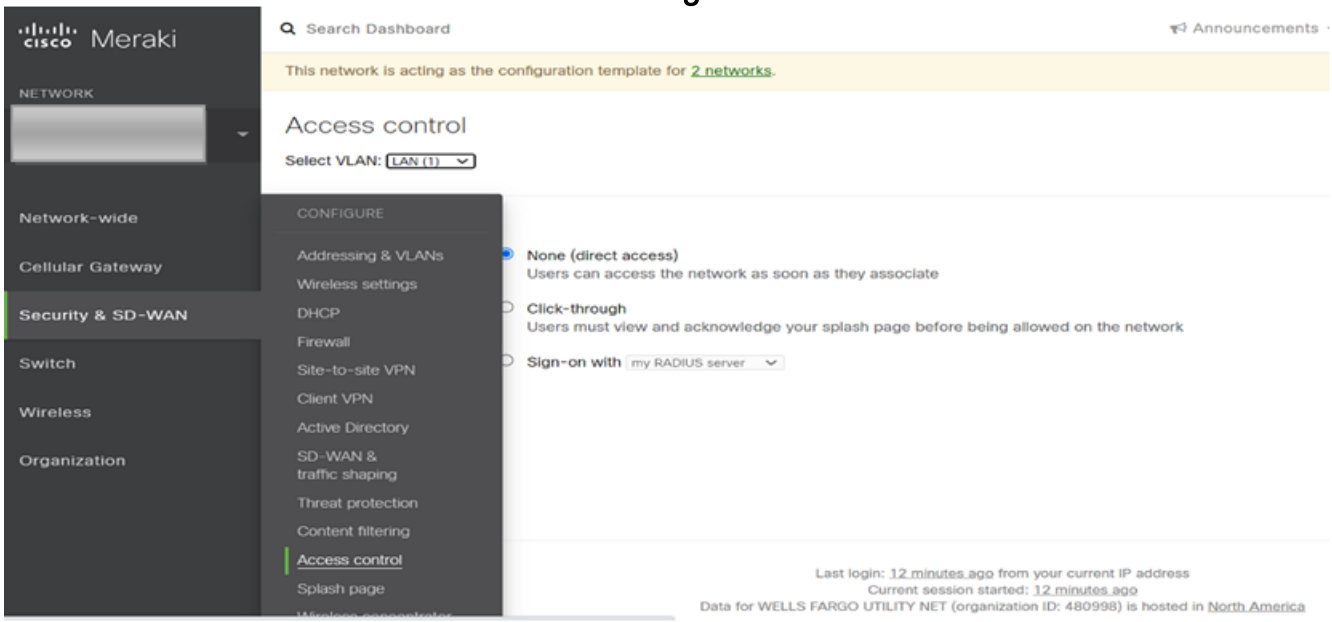
802.1X-Konfiguration

Die 802.1X-RADIUS-Konfiguration finden Sie im angegebenen Pfad, der vom Meraki-Produktmodell abhängt.

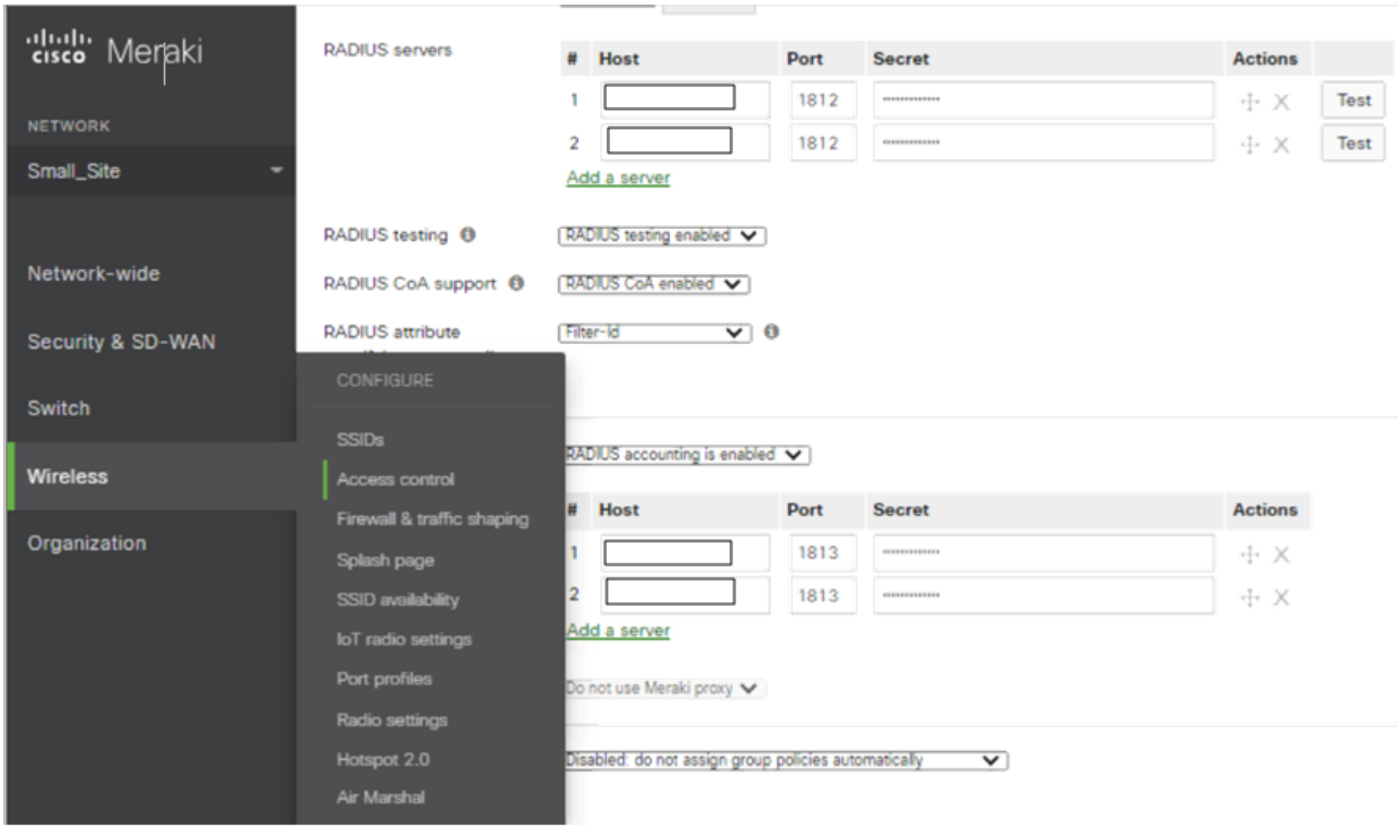
1. MX-Security Appliance (entweder für Access-Ports oder Wireless konfiguriert)

- Für Access-Ports
  Sicherheit und SD-WAN > Adressierung und VLANs

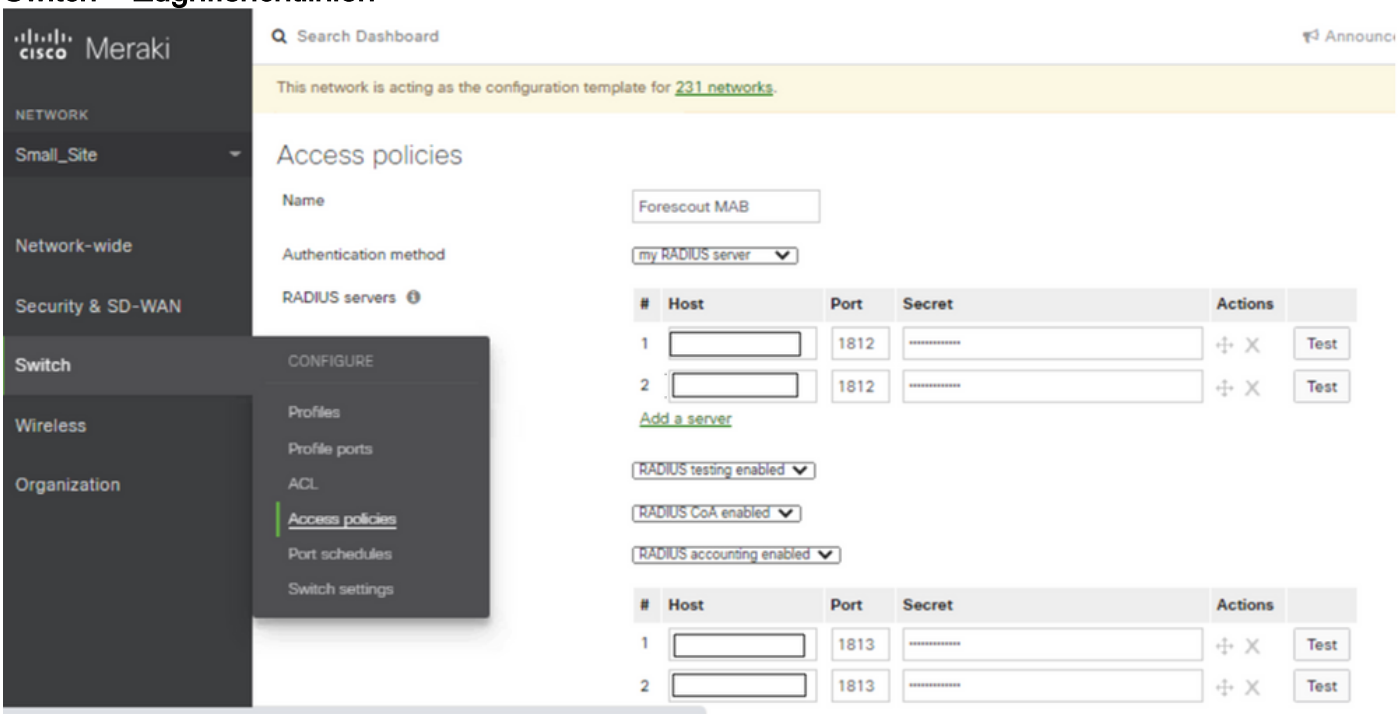
- Für Wireless
  Sicherheits- und SD-WAN > Wireless-Einstellungen



2. MR-Access Points (auf Basis einer Service Set Identifier (SSID) aktiviert):
Wireless > Zugriffskontrolle



3. MS-Switches
Switch > Zugriffsrichtlinien

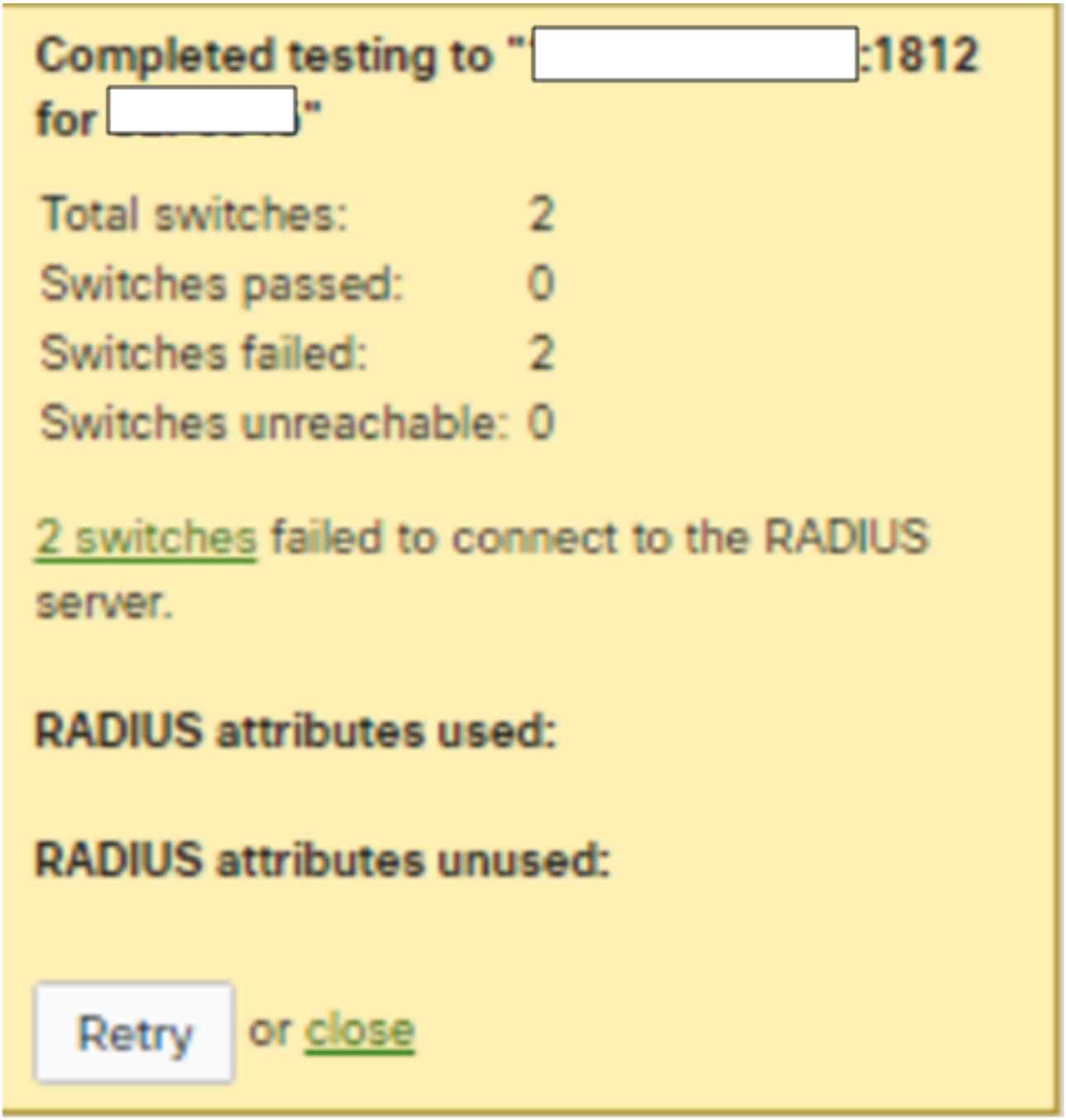


802.1X-Konfigurationsprüfung

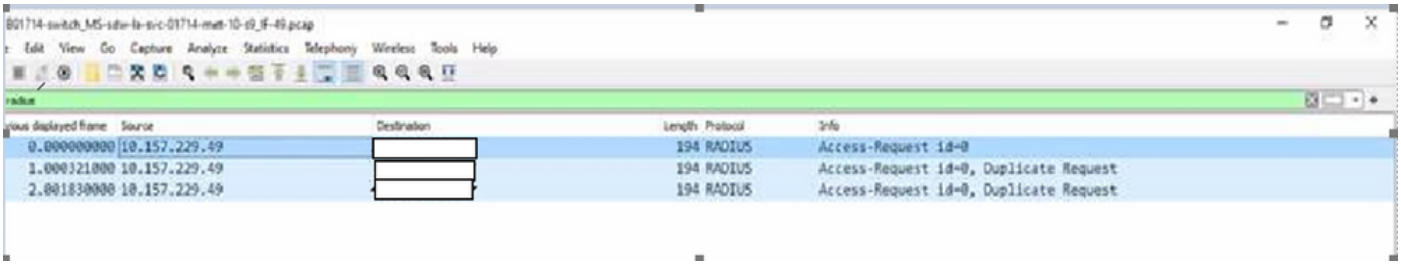
- **Meraki Dashboard > Netzwerkvorlage > Switch > Zugriffsrichtlinien > Radius-Server > Test**
- **Meraki-Dashboard > Netzwerkvorlage > Wireless > Zugriffskontrolle > Radius-Server > Test**

1. Wenn das Testergebnis als **All AP failed to connect radius server (Gesamter Access Point konnte keinen Radius-Server verbinden)** festgestellt wird, müssen Sie überprüfen, wo die access-

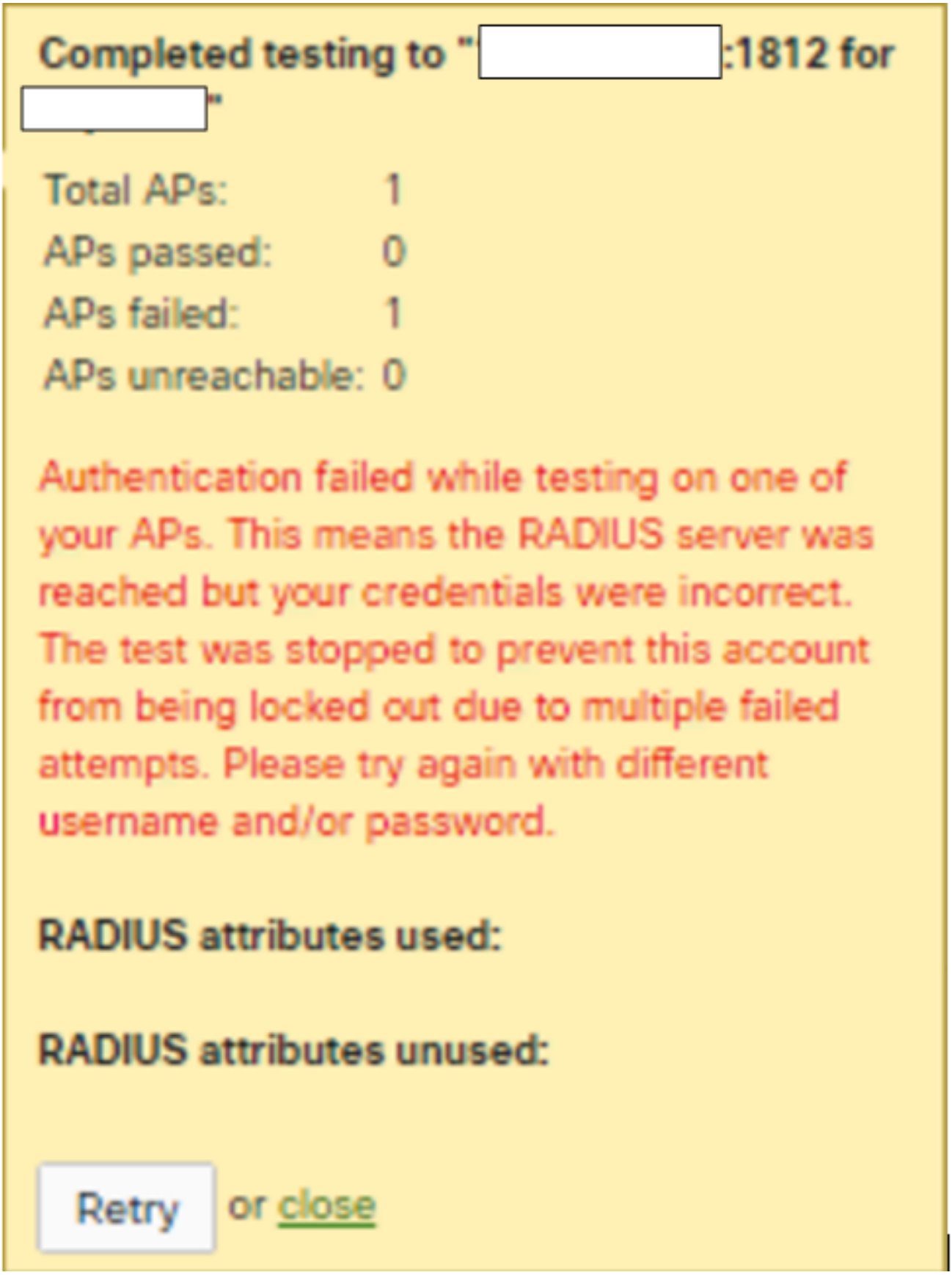
Request verworfen wurde.



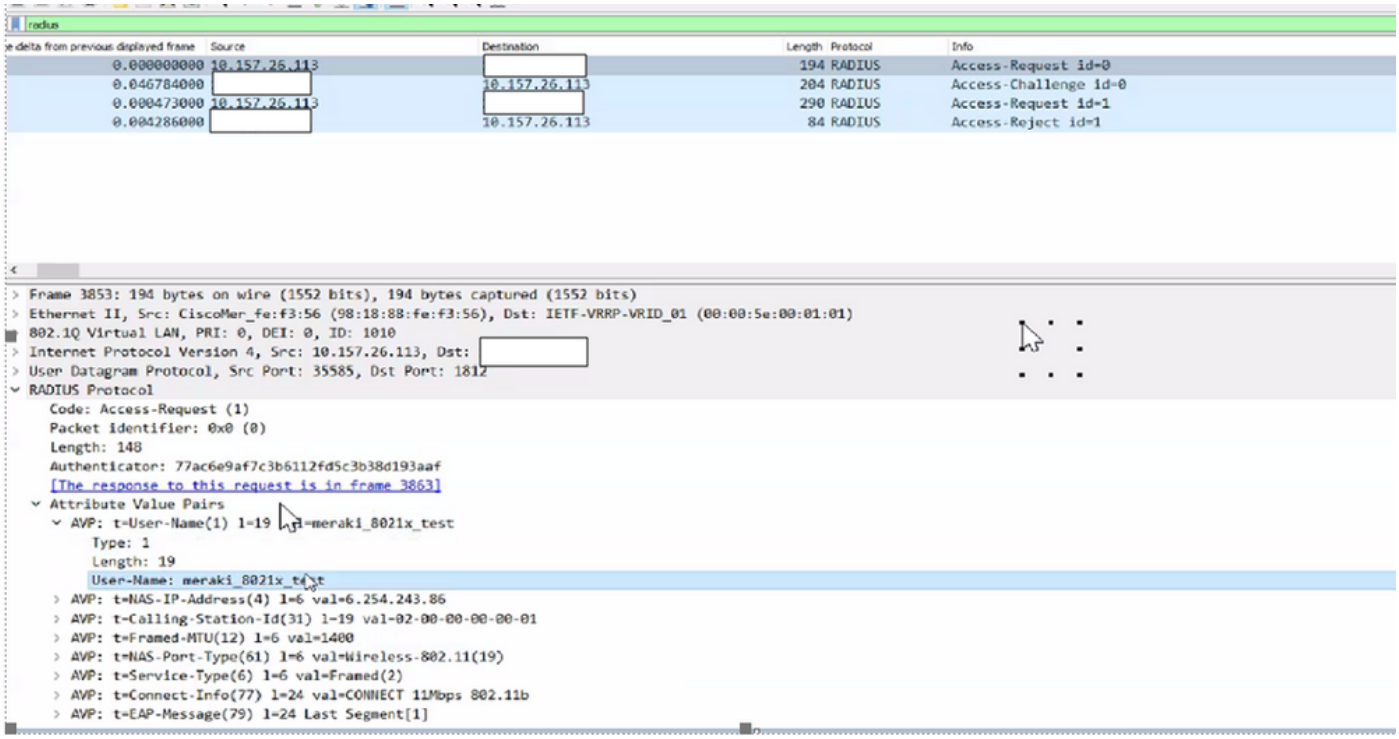
2. Führen Sie die Paketerfassung auf dem Uplink-Port aus, und überprüfen Sie den Fluss der Zugriffsanfragen. Siehe Screenshot des Paketerfassungszugriffs - Die Anfrage erhält keine Antwort.



3. Wird ein Testergebnis als Accept/Ablehnen/Ablehnen/Ablehnen/Antwort/falsche Anmeldeinformationen geantwortet, bedeutet dies, dass der Radius-Server aktiv ist.

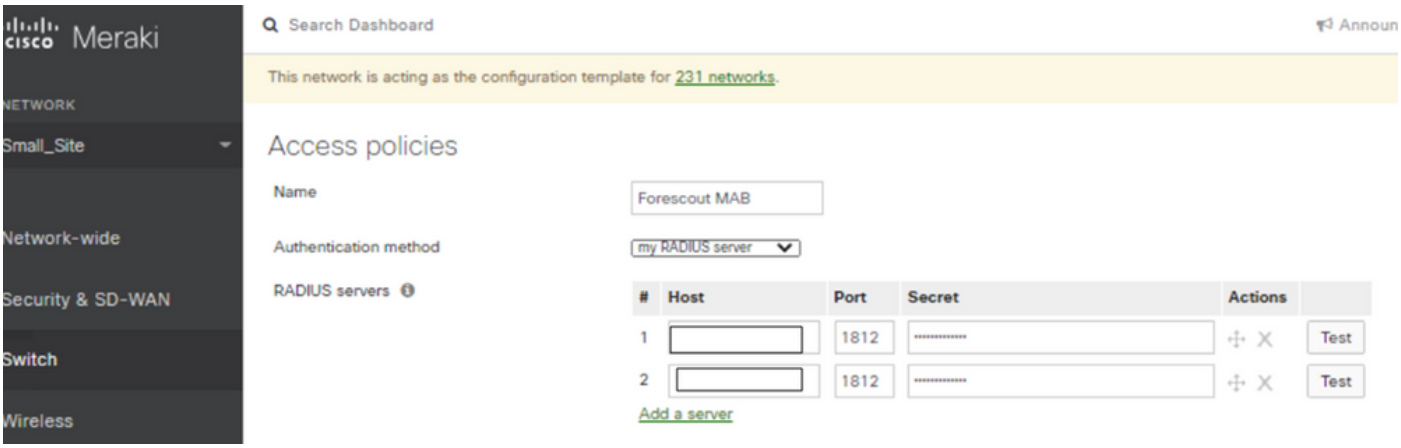


4. Führen Sie die Paketerfassung auf dem Uplink-Port aus, und überprüfen Sie den Fluss der Zugriffsanfragen. Siehe Screenshot des Paketerfassungs-Zugriffs - Die Anfrage erhielt eine Antwort.

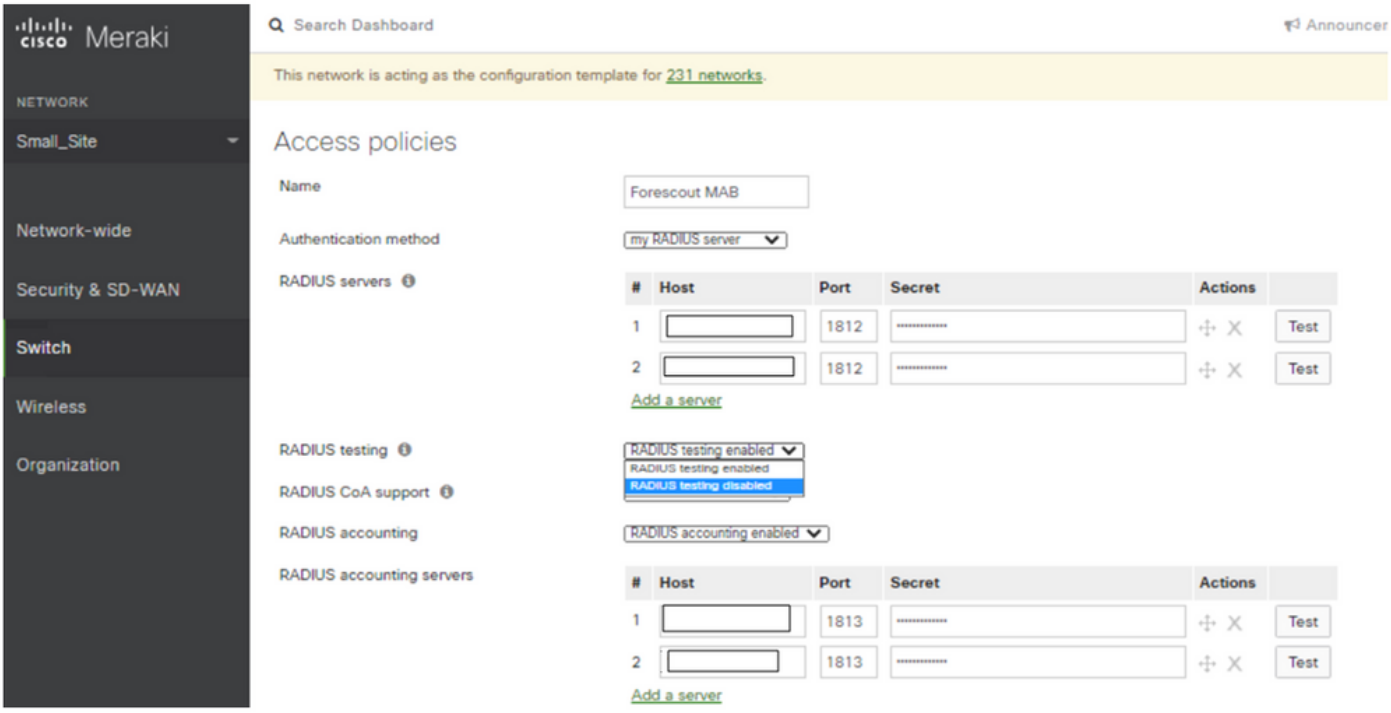


Überprüfung der Zugriffsrichtlinien

1. Überprüfen Sie, ob der in der Zugriffsrichtlinie genannte Parameter korrekt ist und Host-IP, Port-Nummer und geheimer Schlüssel umfasst.



2. Konfigurierte Radius-Server-IPs werden in der Produktion nicht oder nicht verwendet, oder Zugriffsrichtlinien werden nicht verwendet. Es wird empfohlen, die Zugriffsrichtlinie zu entfernen. Wenn Sie diese Einstellung beibehalten möchten, können Sie die **Testeinstellung Radius** deaktivieren.



Zugehörige Informationen

- https://documentation.meraki.com/General_Administration/Cross-Platform_Content/Alert_-_Recent_802.1X_Failure
- Technischer Support und Dokumentation für Cisco Systeme

Hinweis

- Wenn die RADIUS-Server Meraki-Geräte abfragen und den LAN-IP- und Standard-Benutzernamen "meraki_8021x_test" verwenden, verwendete das Meraki-Dashboard die Meraki-MAC-Adresse als Quelle.
- Meraki gab diesen Warnmeldungen seit Oktober 2021 Einblick.