Überprüfen des 802.1X-Client-Ausschlusses auf einem AireOS WLC

Inhalt

Einleitung

In diesem Dokument wird der Ausschluss des 802.1X-Clients auf einem AireOS Wireless LAN Controller (WLC) beschrieben.

Voraussetzungen

Anforderungen

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

- Cisco AireOS WLC
- 802.1X-Protokoll
- RADIUS (Remote Authentication Dial-In User Service)
- Identity Service Engine (ISE)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf AireOS.

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 möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Der 802.1X-Client-Ausschluss ist eine wichtige Option für einen 802.1X-Authentifizierer wie einen WLC. Dadurch soll eine Überlastung der Authentifizierungsserver-Infrastruktur durch EAP-Clients (Extensible Authentication Protocol) verhindert werden, die hyperaktiv sind oder nicht ordnungsgemäß funktionieren.

Anwenderbeispiele

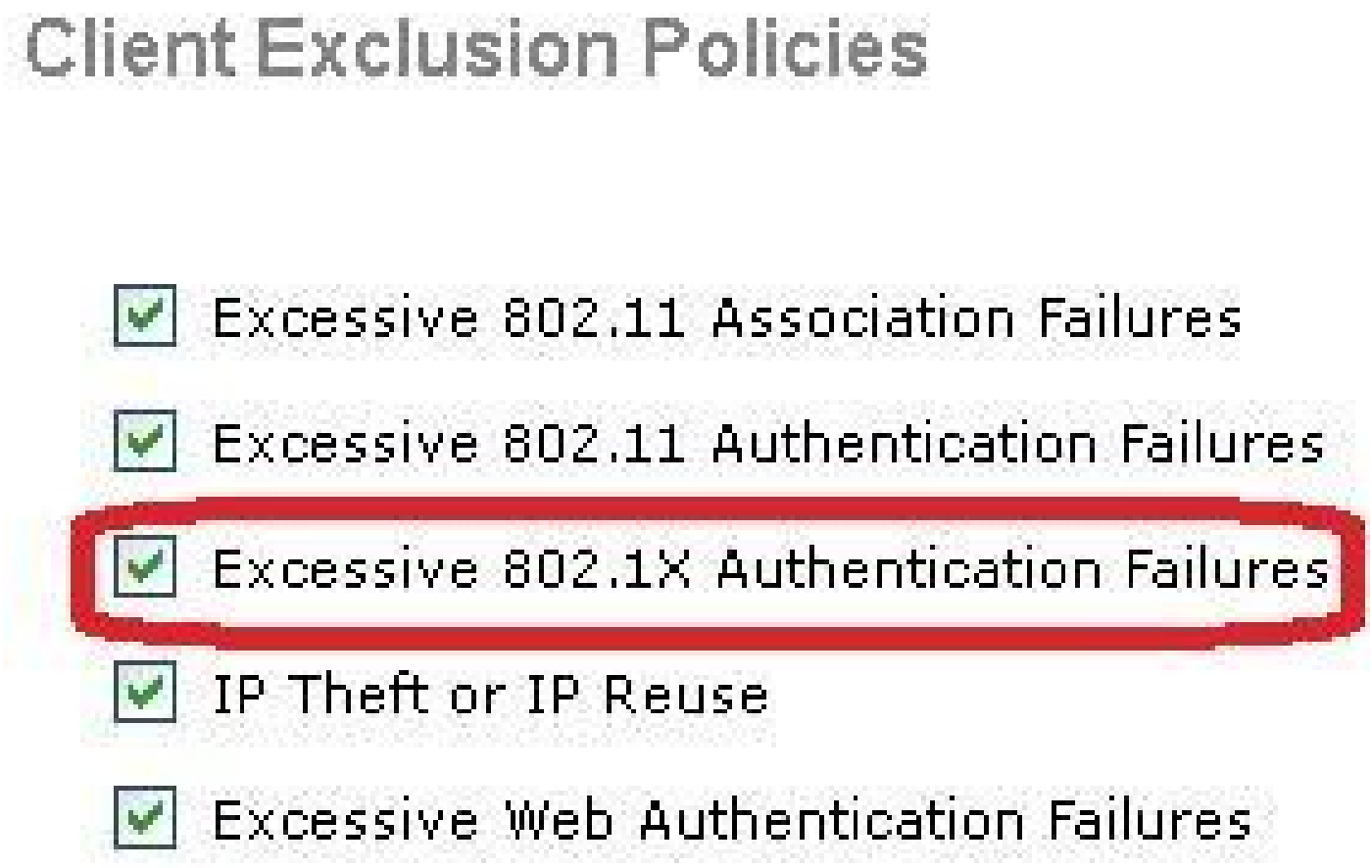
Beispiele für Anwendungsfälle:

- Eine EAP-Komponente, die mit falschen Anmeldeinformationen konfiguriert wurde. Die meisten Supplicants, wie z. B. EAP Supplicants, beenden Authentifizierungsversuche nach einigen aufeinander folgenden Fehlern. Einige EAP-Supplicants versuchen jedoch weiterhin, sich bei einem Fehler erneut zu authentifizieren, und zwar möglicherweise mehrmals pro Sekunde. Einige Clients überlasten RADIUS-Server und verursachen einen Denial of Service (DoS) für das gesamte Netzwerk.
- Nach einem größeren Netzwerk-Failover können Hunderte oder Tausende von EAP-Clients gleichzeitig versuchen, sich zu authentifizieren. Dadurch können die Authentifizierungsserver überlastet werden und eine langsame Reaktion ermöglichen. Wenn die Clients oder der Authentifikator eine Zeitüberschreitung aufweisen, bevor die langsame Antwort verarbeitet wird, kann es zu einem Teufelskreis kommen, bei dem die Authentifizierungsversuche weiterhin eine Zeitüberschreitung verursachen und dann erneut versuchen, die Antwort zu verarbeiten.

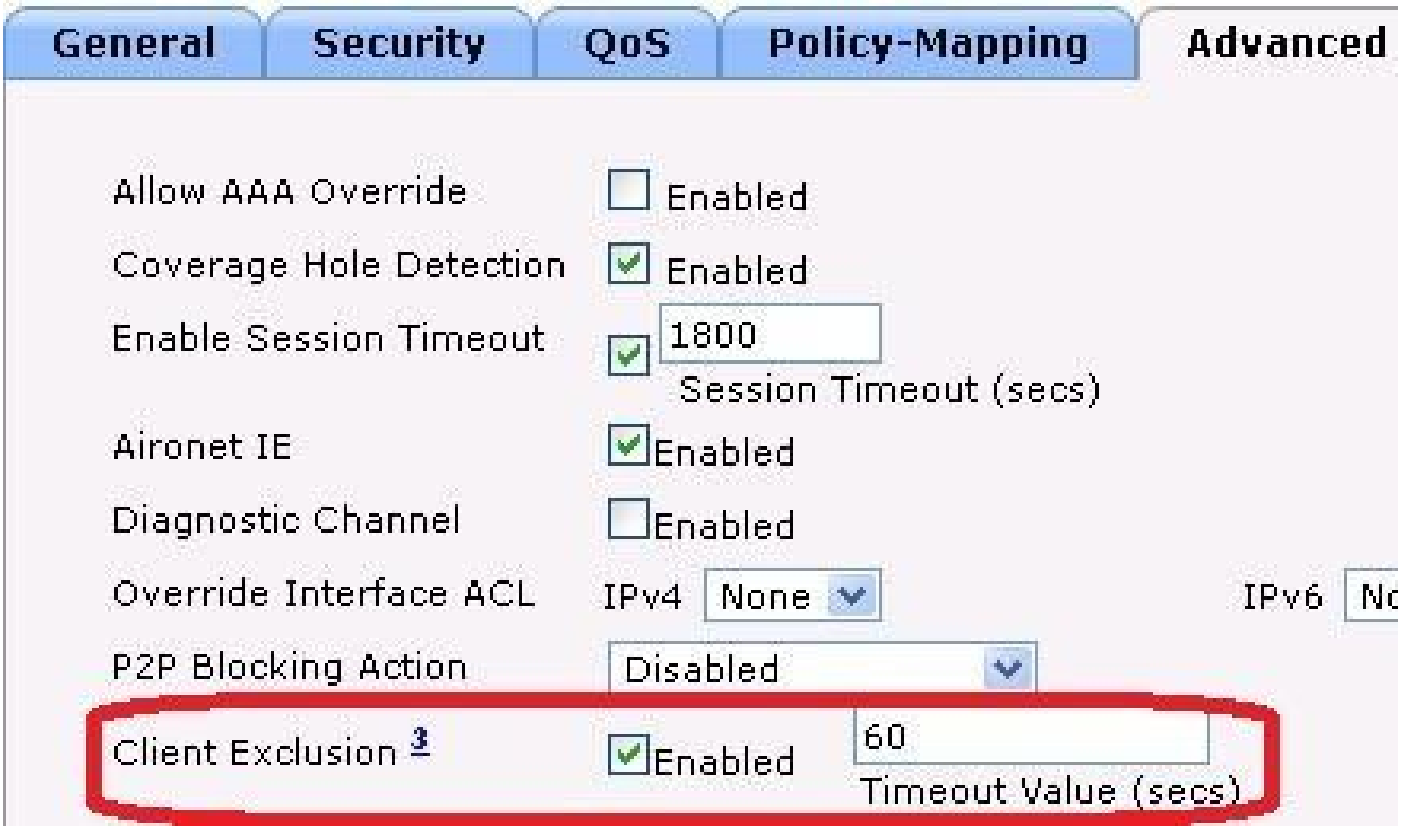
Hinweis: Ein Zugangskontrollmechanismus ist erforderlich, damit Authentifizierungsversuche erfolgreich sind.

So funktioniert der 802.1x-Client-Ausschluss?

Der 802.1X-Clientausschluss verhindert, dass Clients nach übermäßigem 802.1X-Authentifizierungsfehler über einen längeren Zeitraum Authentifizierungsversuche senden. Auf einem AireOS WLC 802.1X wird der Client-Ausschluss global aktiviert, indem Sie standardmäßig zu Security > Wireless Protection Policies > Client Exclusion Policies navigieren und in diesem Bild angezeigt werden.



Der Client-Ausschluss kann für jedes WLAN aktiviert oder deaktiviert werden. Standardmäßig ist sie mit einer Zeitüberschreitung von 60 Sekunden vor AireOS 8.5 und 180 Sekunden ab AireOS 8.5 aktiviert.



Ausschlusseinstellungen zum Schutz von RADIUS-Servern vor Überlastung

Um sicherzustellen, dass der RADIUS-Server vor Überlastung durch fehlerhaft funktionierende Wireless-Clients geschützt ist, überprüfen Sie, ob die folgenden Einstellungen gültig sind:

- Übermäßige 802.1X-Authentifizierungsfehler werden in den globalen Client-Ausschlussrichtlinien des WLC ausgewählt.
- In den erweiterten WLAN-Einstellungen ist die Option "Client Exclusion" aktiviert.
- Der Wert für das Clientausschlusstimeout ist auf 60 bis 300 Sekunden festgelegt.

> Hinweis: Werte über 300 Sekunden bieten besseren Schutz, können jedoch Benutzerbeschwerden auslösen.

- Konfigurieren von AireOS-EAP-Timern und ISE Protected Extensible Authentication Protocol (PEAP)-Einstellungen

Probleme, die verhindern, dass der 802.1x-Ausschluss funktioniert

Mehrere Konfigurationseinstellungen im WLC und im RADIUS-Server können verhindern, dass der 802.1X-Client-Ausschluss funktioniert.

Clients aufgrund von WLC-EAP-Timer-Einstellungen nicht ausgeschlossen

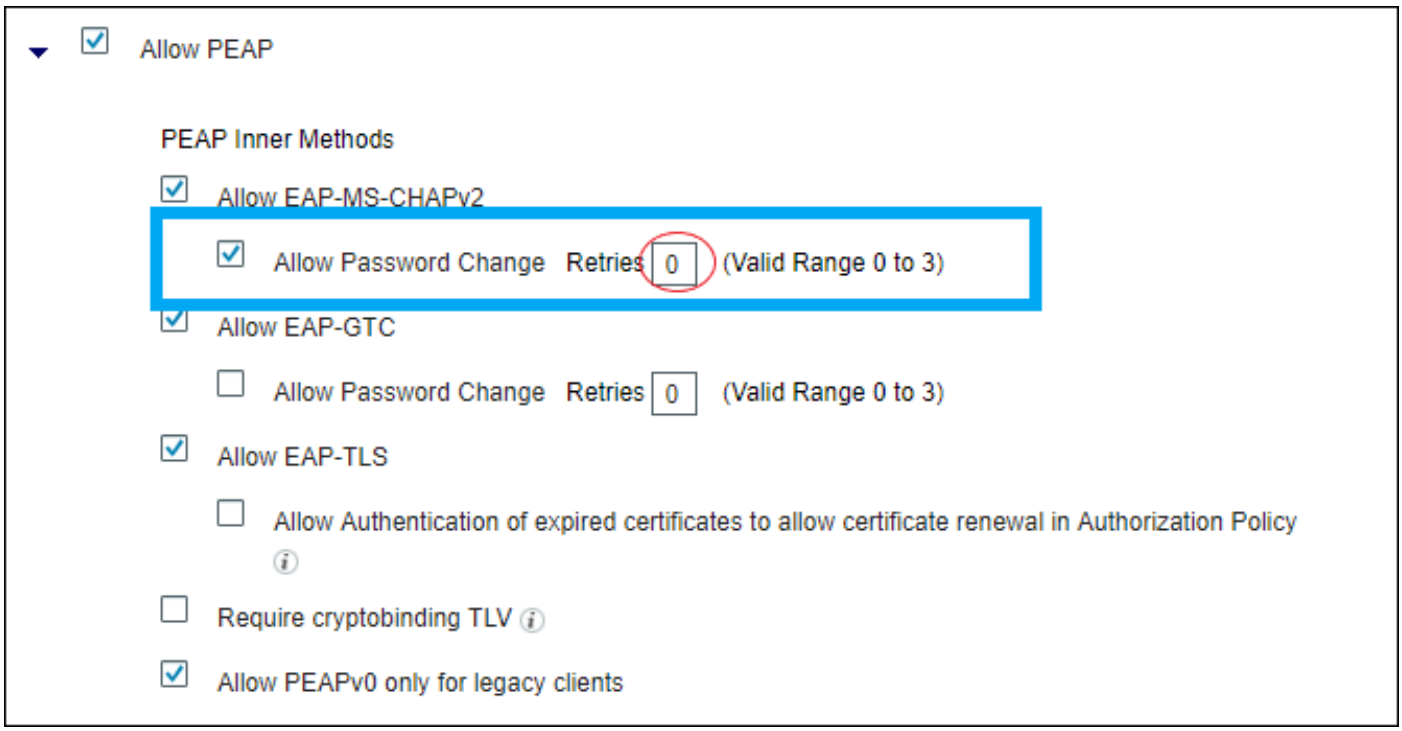
Standardmäßig sind Wireless-Clients nicht ausgeschlossen, wenn Client Exclusion im WLAN auf Enabled (Aktiviert) festgelegt ist. Dies liegt an langen Standard-EAP-Zeitüberschreitungen von 30 Sekunden, die dazu führen, dass ein fehlerhafter Client niemals genügend Fehler in Folge bekommt, um einen Ausschluss auszulösen. Konfigurieren Sie kürzere EAP-Zeitüberschreitungen mit einer höheren Anzahl von Neuübertragungen, damit der 802.1X-Client-Ausschluss wirksam wird. Siehe das Beispiel mit der Zeitüberschreitung.

```
config advanced eap identity-request-timeout 3
config advanced eap identity-request-retries 10
config advanced eap request-timeout 3
config advanced eap request-retries 10
```

Clients aufgrund von ISE PEAP-Einstellungen nicht ausgeschlossen

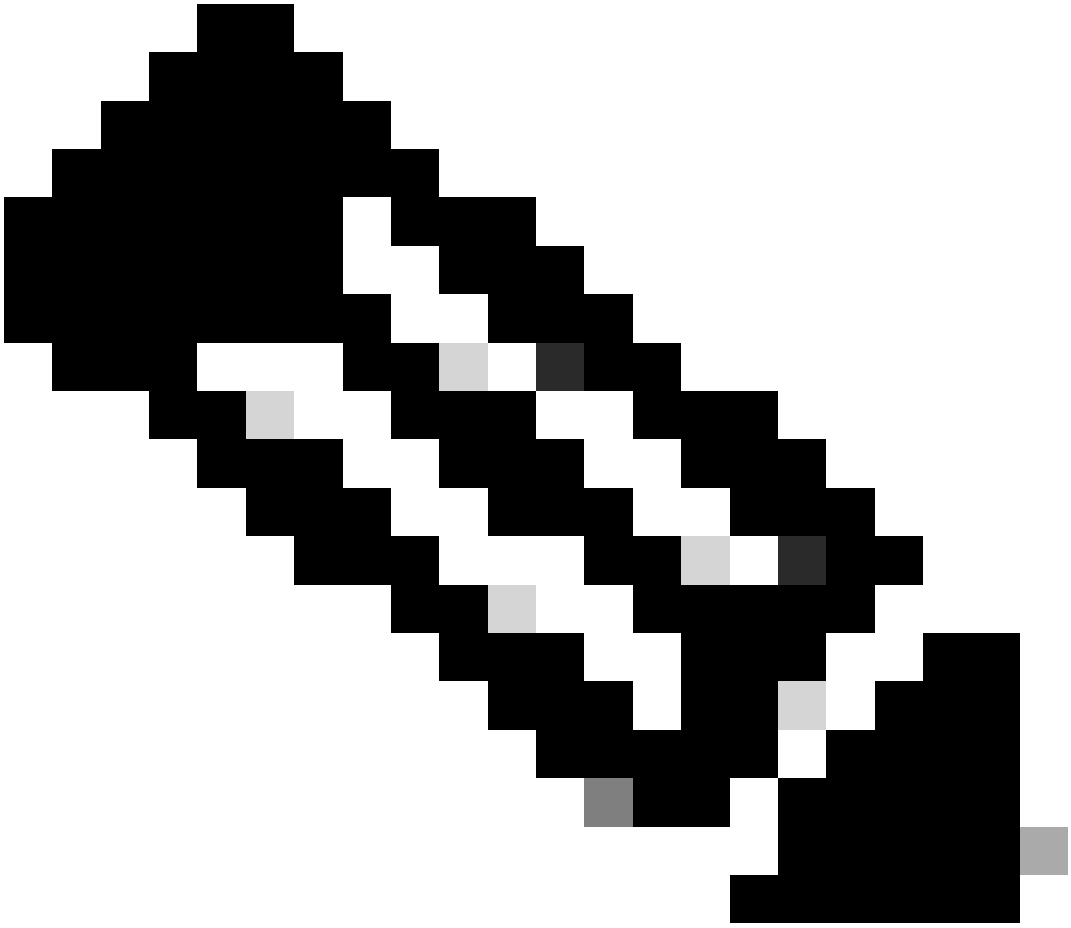
Damit der 802.1X-Client-Ausschluss funktioniert, muss der RADIUS-Server eine Access-Reject-

Nachricht senden, wenn die Authentifizierung fehlschlägt. Wenn der RADIUS-Server ISE ist und PEAP verwendet wird, kann kein Ausschluss erfolgen, und dies hängt von den ISE-PEAP-Einstellungen ab. Navigieren Sie in der ISE zu Policy > Results > Authentication > Allowed Protocols > Default Network Access, wie im Bild dargestellt.



Wenn Sie Retries (rechts rot eingekreist) auf 0 setzen, muss die ISE Access-Reject sofort an den WLC senden, der den WLC aktivieren muss, um den Client auszuschließen (wenn er dreimal versucht, sich zu authentifizieren).

Hinweis: Die Einstellung für Wiederholungen ist etwas unabhängig vom Kontrollkästchen Kennwortänderung zulassen, d. h., der Wert für Wiederholungen kann berücksichtigt werden, auch wenn Kennwortänderung zulassen deaktiviert ist. Wenn Retries jedoch auf 0 gesetzt ist, funktioniert Kennwortänderung zulassen nicht.



Hinweis: Weitere Informationen finden Sie unter Cisco Bug ID CSCsq16858. Nur registrierte Cisco Benutzer können auf Bug-Tools und Informationen von Cisco zugreifen.

Zugehörige Informationen

- Verhinderung umfangreicher Netzwerkzusammenbrüche bei Wireless RADIUS-Netzwerken
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.