Konfigurieren von CWA mit FlexConnect APs auf einem WLC mit ISE

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die zentrale Webauthentifizierung mit FlexConnect Access Points (APs) auf einem Wireless LAN Controller (WLC) mit Identity Services Engine (ISE) im lokalen Switching-Modus konfiguriert wird.

Wichtiger Hinweis: Derzeit wird die lokale Authentifizierung auf den FlexAPs in diesem Szenario nicht unterstützt.

Weitere Dokumente dieser Serie

- Konfigurationsbeispiel für die zentrale Web-Authentifizierung mit Switch und Identity Services Engine
- Zentrale Webauthentifizierung im Konfigurationsbeispiel für WLC und ISE

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Services Engine (ISE) Version 1.2.1
- Wireless LAN Controller-Software, Release-Version - 7.4.100.0

Konfigurieren

Es gibt mehrere Methoden, um die zentrale Webauthentifizierung auf dem Wireless LAN Controller (WLC) zu konfigurieren. Die erste Methode ist die lokale Web-Authentifizierung, bei der der WLC den HTTP-Datenverkehr an einen internen oder externen Server umleitet, wo der Benutzer zur Authentifizierung aufgefordert wird. Der WLC ruft dann die Anmeldeinformationen ab (im Fall eines externen Servers über eine HTTP GET-Anforderung zurückgesendet) und führt eine RADIUS-Authentifizierung durch. Bei einem Gastbenutzer ist ein externer Server (z. B. Identity Service Engine (ISE) oder NAC Guest Server (NGS)) erforderlich, da das Portal Funktionen wie die Geräteregistrierung und die benutzerseitige Bereitstellung bereitstellt. Dieser Prozess umfasst folgende Schritte:

1. Der Benutzer wird der Webauthentifizierungs-SSID zugewiesen.
2. Der Benutzer öffnet seinen Browser.
3. Der WLC leitet direkt nach Eingabe einer URL zum Gastportal (z. B. zur ISE oder zum NGS) weiter.
4. Der Benutzer authentifiziert sich im Portal.
5. Das Gastportal leitet mit den eingegebenen Anmeldeinformationen zurück zum WLC.
6. Der WLC authentifiziert den Gastbenutzer über RADIUS.
7. Der WLC kehrt zur ursprünglichen URL zurück.

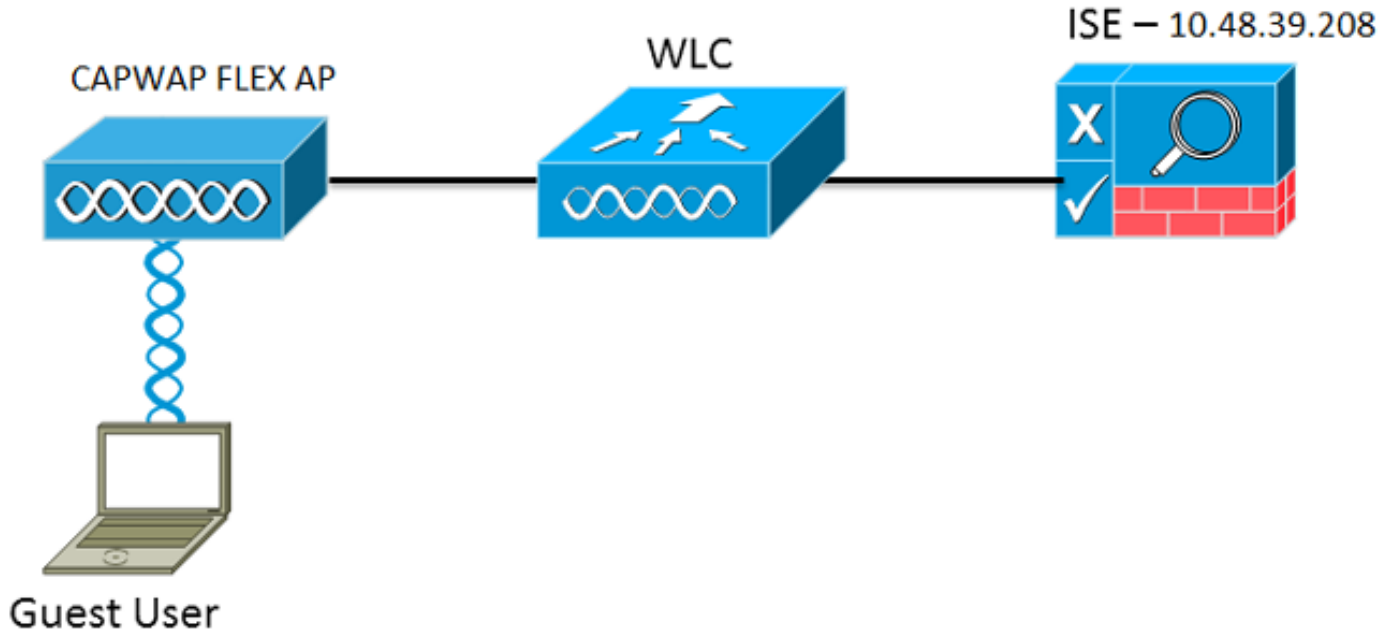
Dieser Prozess beinhaltet eine Menge Umleitung. Der neue Ansatz besteht in der zentralen Web-Authentifizierung, die mit ISE (Versionen später als 1.1) und WLC (Versionen später als 7.2) funktioniert. Dieser Prozess umfasst folgende Schritte:

1. Der Benutzer wird der Webauthentifizierungs-SSID zugewiesen.
2. Der Benutzer öffnet seinen Browser.
3. Der WLC leitet zum Gastportal um.
4. Der Benutzer authentifiziert sich im Portal.
5. Die ISE sendet eine RADIUS-Autorisierungsänderung (CoA - UDP-Port 1700), um dem Controller die Gültigkeit des Benutzers anzuzeigen, und überträgt schließlich RADIUS-Attribute wie die Zugriffskontrollliste (ACL).
6. Der Benutzer wird aufgefordert, die ursprüngliche URL erneut zu versuchen.

In diesem Abschnitt werden die erforderlichen Schritte zum Konfigurieren der zentralen Webauthentifizierung auf dem WLC und der ISE beschrieben.

Netzwerkdiagramm

Bei dieser Konfiguration wird folgende Netzwerkkonfiguration verwendet:

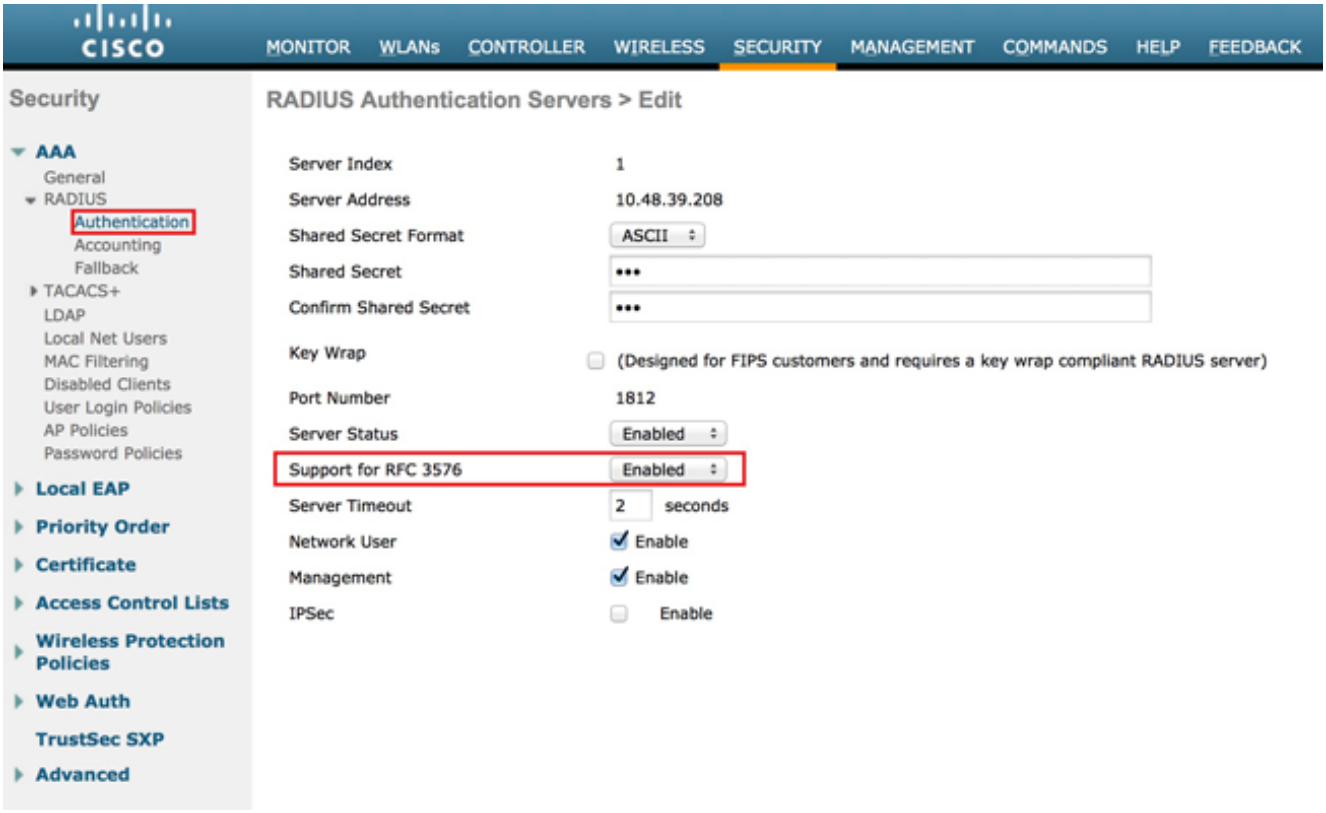


WLC-Konfiguration

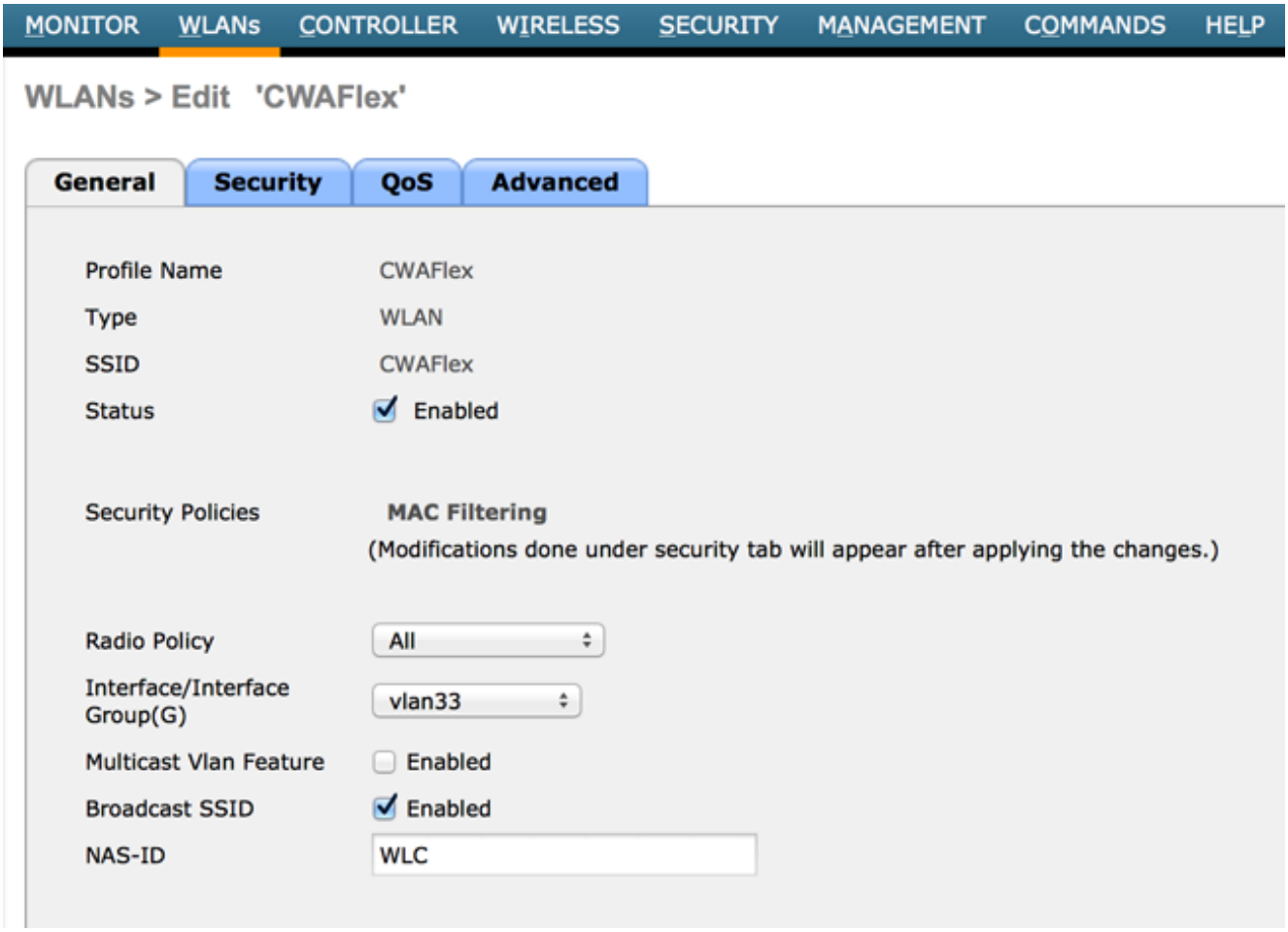
Die WLC-Konfiguration ist relativ einfach. Ein "Trick?" wird verwendet (wie bei Switches), um die dynamische Authentifizierungs-URL von der ISE abzurufen. (Da sie CoA verwendet, muss eine Sitzung erstellt werden, da die Sitzungs-ID Teil der URL ist.) Die SSID ist so konfiguriert, dass sie die MAC-Filterung verwendet, und die ISE ist so konfiguriert, dass sie eine Access-Accept-Nachricht zurückgibt, auch wenn die MAC-Adresse nicht gefunden wurde, sodass sie die Umleitungs-URL für alle Benutzer sendet.

Außerdem müssen RADIUS Network Admission Control (NAC) und AAA Override aktiviert sein. Mit RADIUS NAC kann die ISE eine CoA-Anforderung senden, die anzeigt, dass der Benutzer nun authentifiziert ist und auf das Netzwerk zugreifen kann. Es wird auch für Statusüberprüfungen verwendet, bei denen die ISE das Benutzerprofil basierend auf dem Statusergebnis ändert.

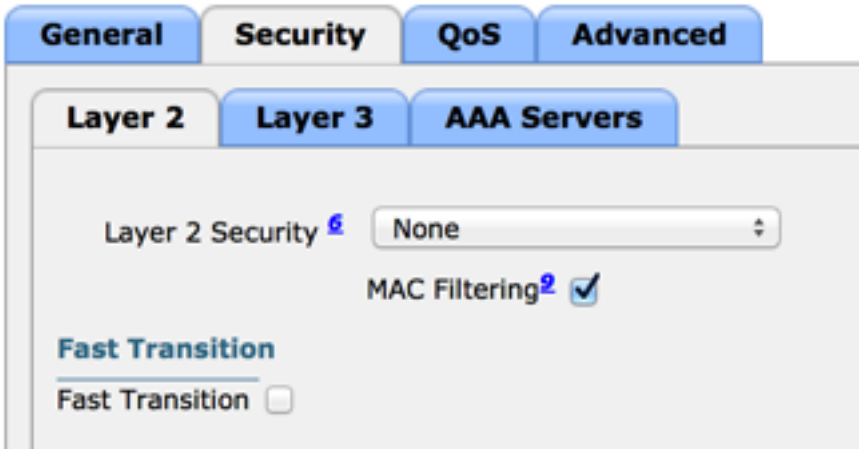
1. Stellen Sie sicher, dass auf dem RADIUS-Server standardmäßig RFC3576 (CoA) aktiviert ist.



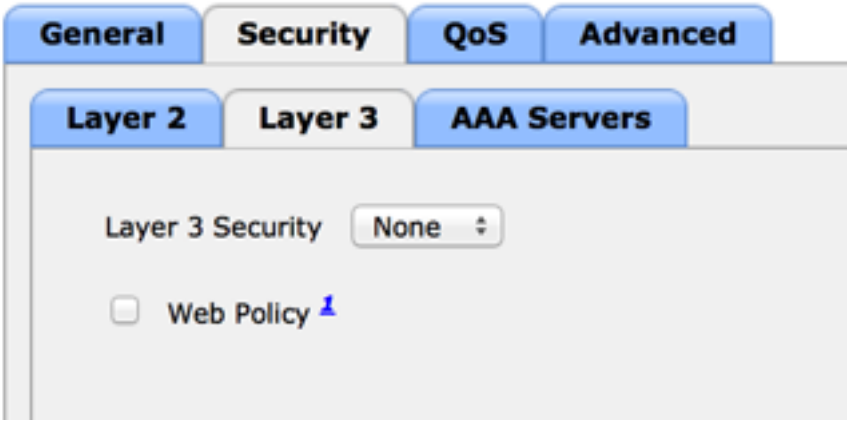
2. Erstellen Sie ein neues WLAN. In diesem Beispiel wird ein neues WLAN mit dem Namen *CWAFlex* erstellt und vlan33 zugewiesen. (Beachten Sie, dass dies keine großen Auswirkungen hat, da sich der Access Point im lokalen Switching-Modus befindet.)



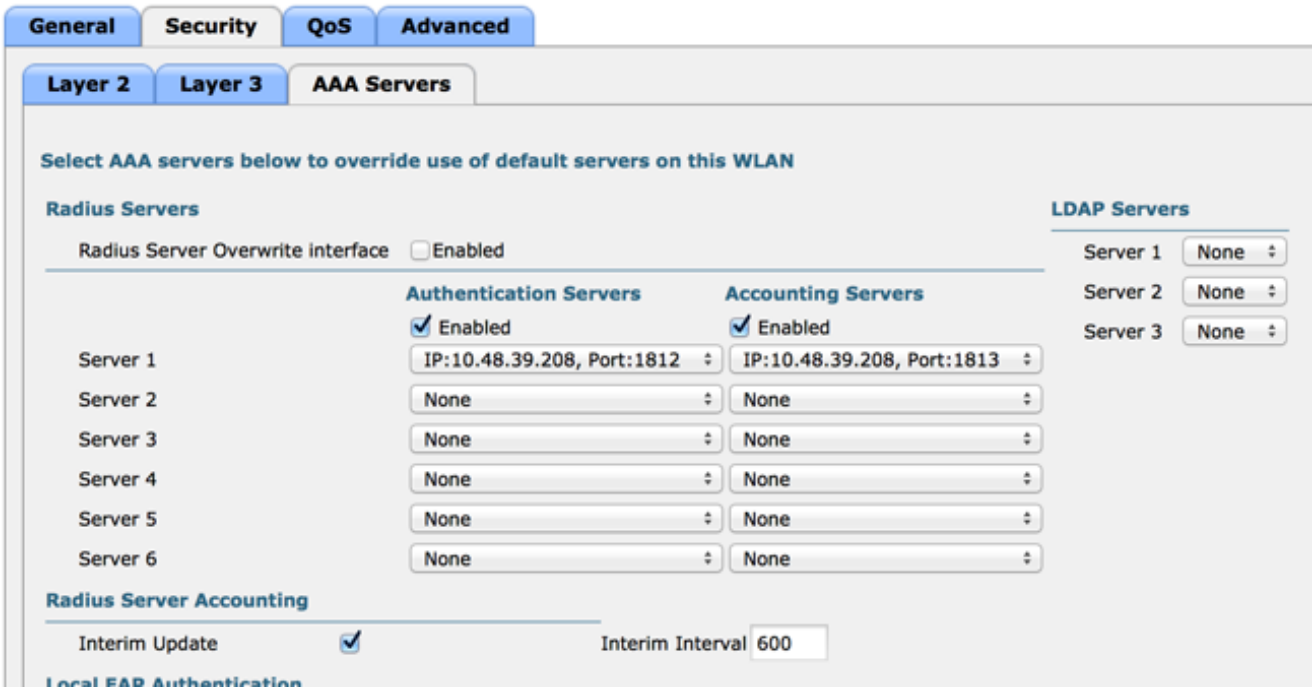
3. Aktivieren Sie auf der Registerkarte Sicherheit die Option MAC-Filterung als Layer-2-Sicherheit.



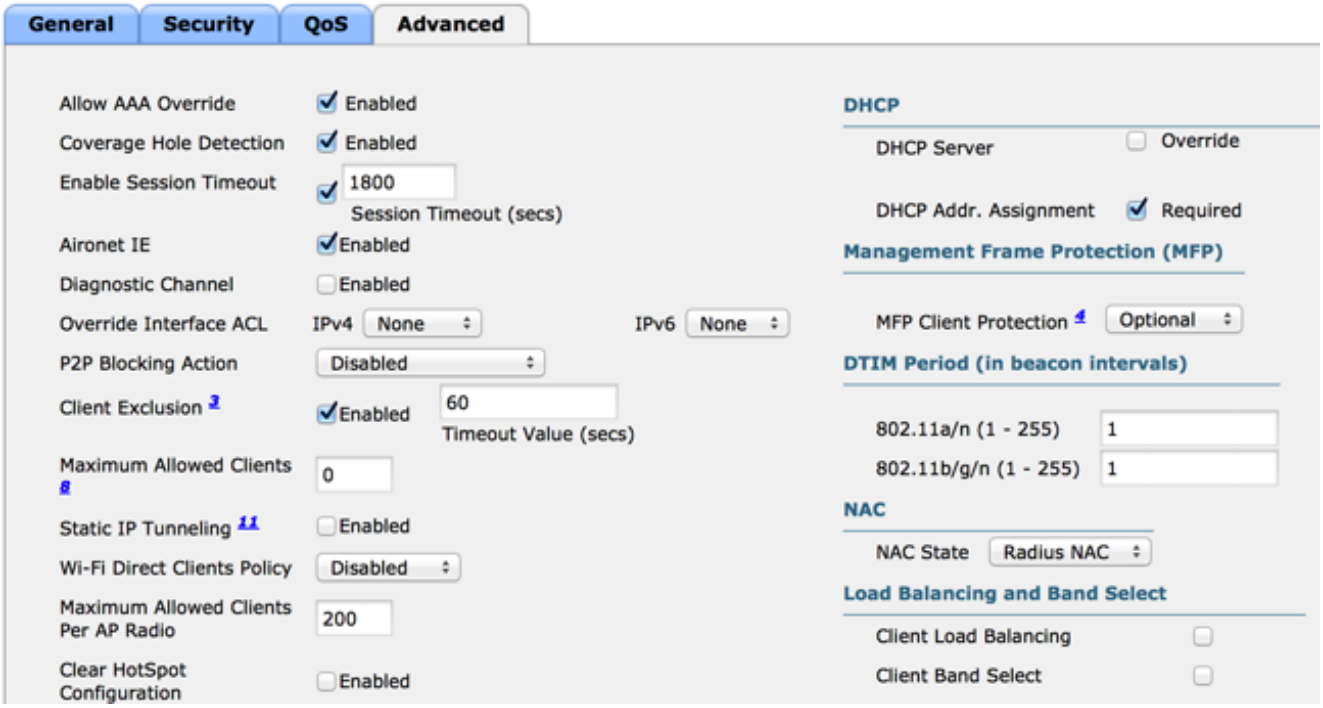
4. Stellen Sie auf der Registerkarte Layer 3 sicher, dass die Sicherheitsfunktion deaktiviert ist. (Wenn die Webauthentifizierung auf Layer 3 aktiviert ist, ist die lokale Webauthentifizierung aktiviert, nicht die zentrale Webauthentifizierung.)



5. Wählen Sie auf der Registerkarte AAA-Server den ISE-Server als Radius-Server für das WLAN aus. Optional können Sie es für die Buchhaltung auswählen, um detailliertere Informationen zur ISE zu erhalten.



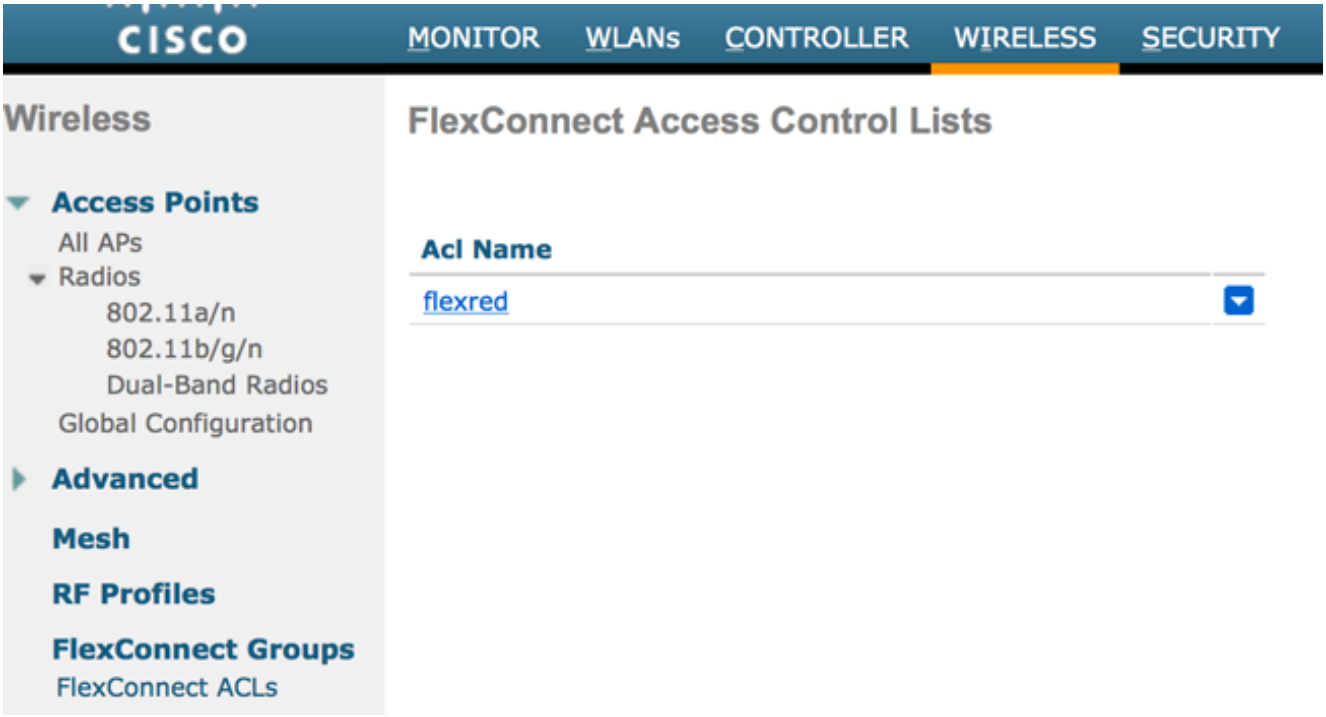
6. Vergewissern Sie sich auf der Registerkarte Advanced, dass Allow AAA Override (AAA-Außerkraftsetzung zulassen) aktiviert ist und Radius NAC für NAC State (NAC-Status) ausgewählt ist.



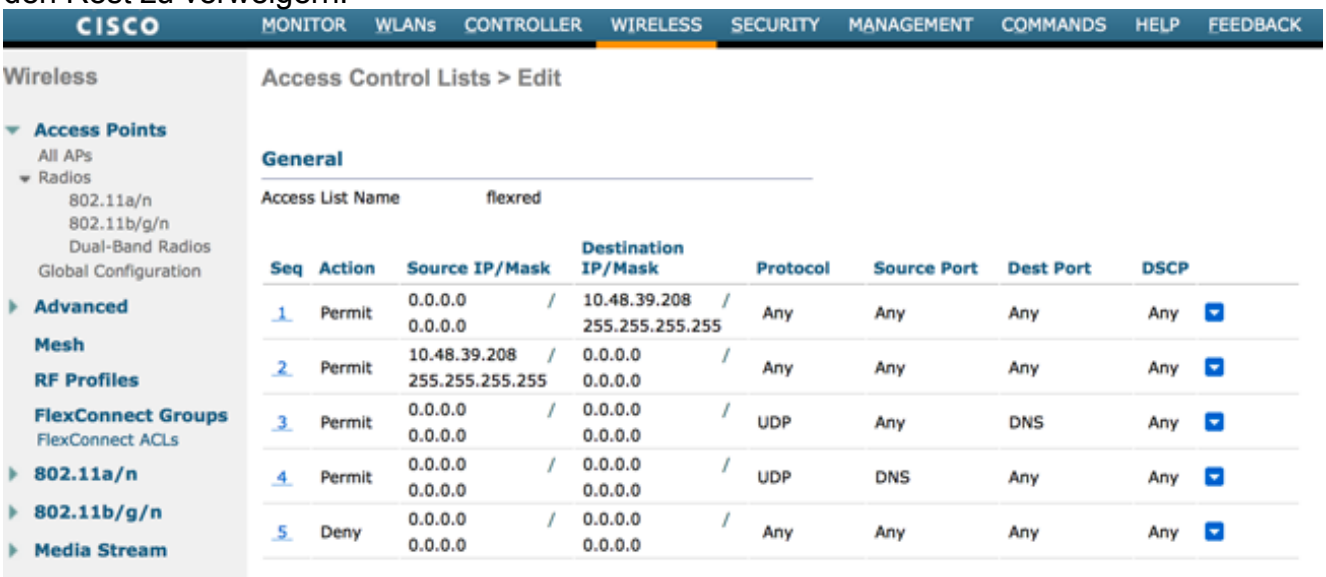
7. Erstellen Sie eine Umleitungszugriffskontrollliste.

Diese ACL wird in der Access-Accept-Nachricht der ISE referenziert und definiert, welcher Datenverkehr umgeleitet (von der ACL abgelehnt) und welcher Datenverkehr nicht umgeleitet werden soll (von der ACL zugelassen). Grundsätzlich müssen DNS und Datenverkehr zur/von der ISE zugelassen werden. **Hinweis**: Ein Problem bei FlexConnect-APs besteht darin, dass Sie eine FlexConnect-ACL erstellen müssen, die von Ihrer normalen ACL getrennt ist. Dieses Problem wurde in Cisco Bug CSCue68065 dokumentiert und in Version 7.5 behoben. In WLC 7.5 und höher ist nur eine FlexACL erforderlich, und es ist

keine Standard-ACL erforderlich. Der WLC erwartet, dass es sich bei der von der ISE zurückgegebenen Umleitungs-ACL um eine normale ACL handelt. Damit dies funktioniert, benötigen Sie jedoch dieselbe ACL, die auch auf die FlexConnect ACL angewendet wird. Dieses Beispiel zeigt, wie Sie eine FlexConnect-ACL mit dem Namen *flexred* erstellen:

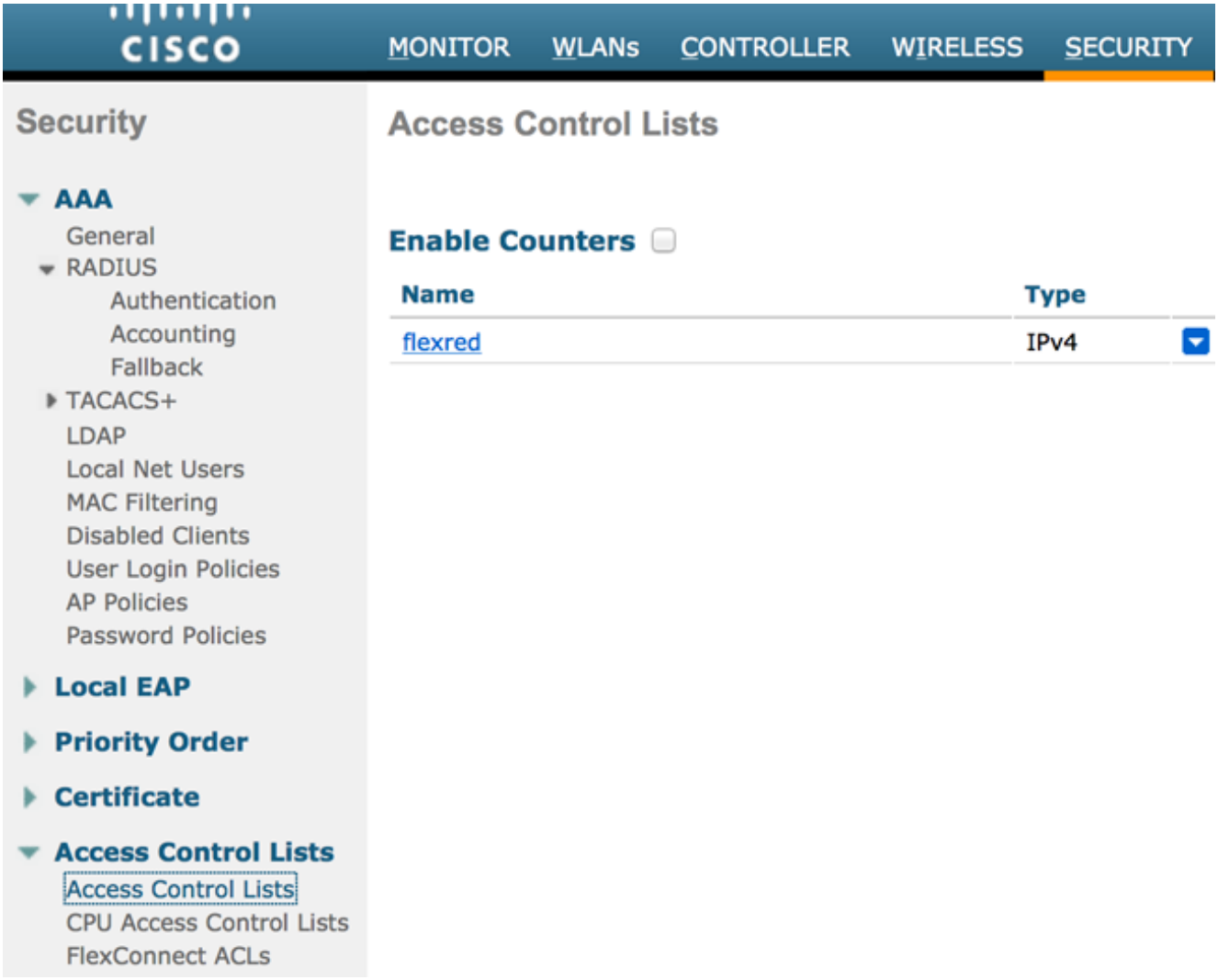


Erstellen Sie Regeln, um DNS-Datenverkehr sowie Datenverkehr zur ISE zuzulassen und den Rest zu verweigern.



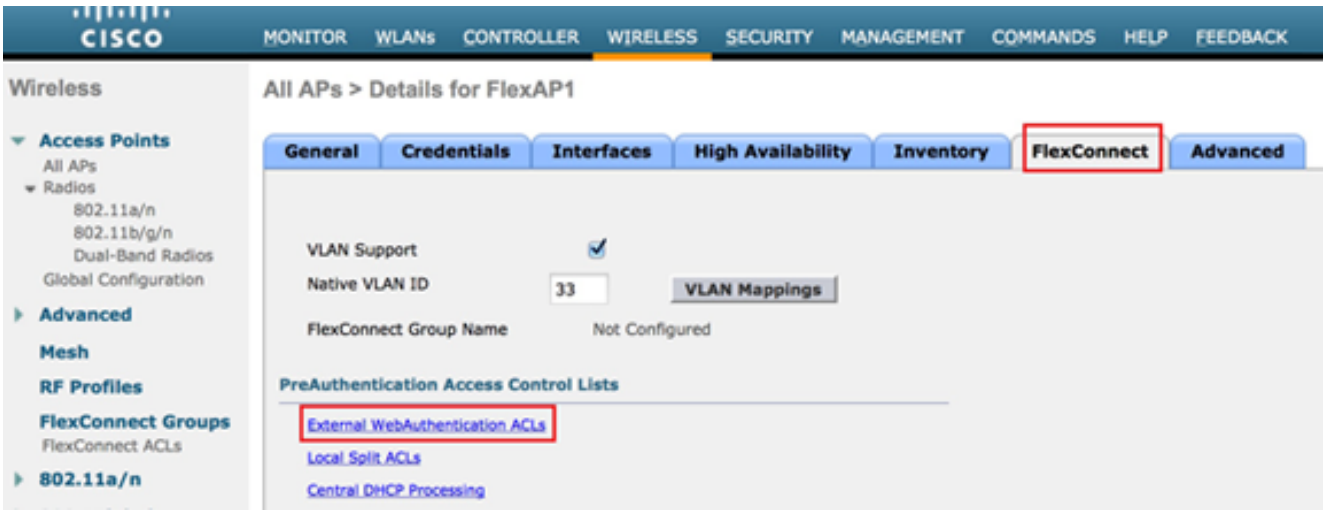
Wenn Sie die maximale Sicherheit wünschen, können Sie nur Port 8443 zur ISE zulassen. (Wenn Sie einen Status erhalten, müssen Sie typische Status-Ports hinzufügen, z. B. 8905.8906.8909.8910.)

(Nur bei Code vor Version 7.5 aufgrund von CSCue68065) Wählen Sie **Security > Access Control Lists (Sicherheit > Zugriffskontrolllisten)**, um eine identische ACL mit demselben Namen zu erstellen.



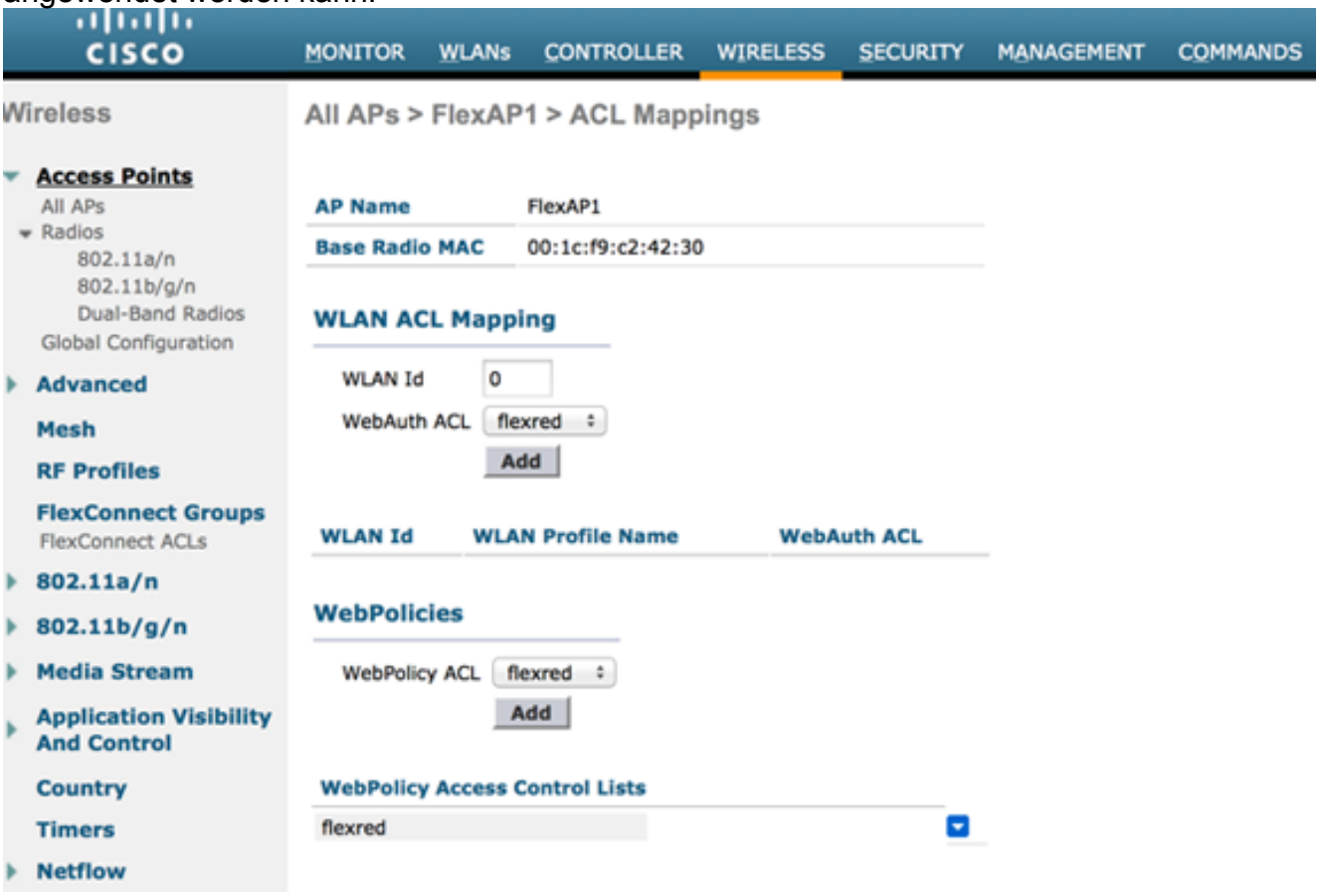
Vorbereiten des jeweiligen FlexConnect AP Beachten Sie, dass Sie bei einer größeren Bereitstellung in der Regel FlexConnect-Gruppen verwenden und diese Elemente aus Gründen der Skalierbarkeit nicht auf AP-Basis ausführen.

Klicken Sie auf **Wireless**, und wählen Sie den gewünschten Access Point aus.Klicken Sie auf die Registerkarte **FlexConnect** und dann auf **Externe Webauthentifizierungs-ACLs**. (Vor Version 7.4 wurde diese Option als *Webrichtlinien* bezeichnet.)



Fügen Sie die ACL (in diesem Beispiel als *flexred* bezeichnet) zum Bereich für Webrichtlinien

hinzu. Dadurch wird die ACL vorab an den Access Point übertragen. Sie wird noch nicht angewendet, aber der ACL-Inhalt wird an den Access Point übergeben, damit er bei Bedarf angewendet werden kann.



Die WLC-Konfiguration ist jetzt abgeschlossen.

ISE-Konfiguration

Autorisierungsprofil erstellen

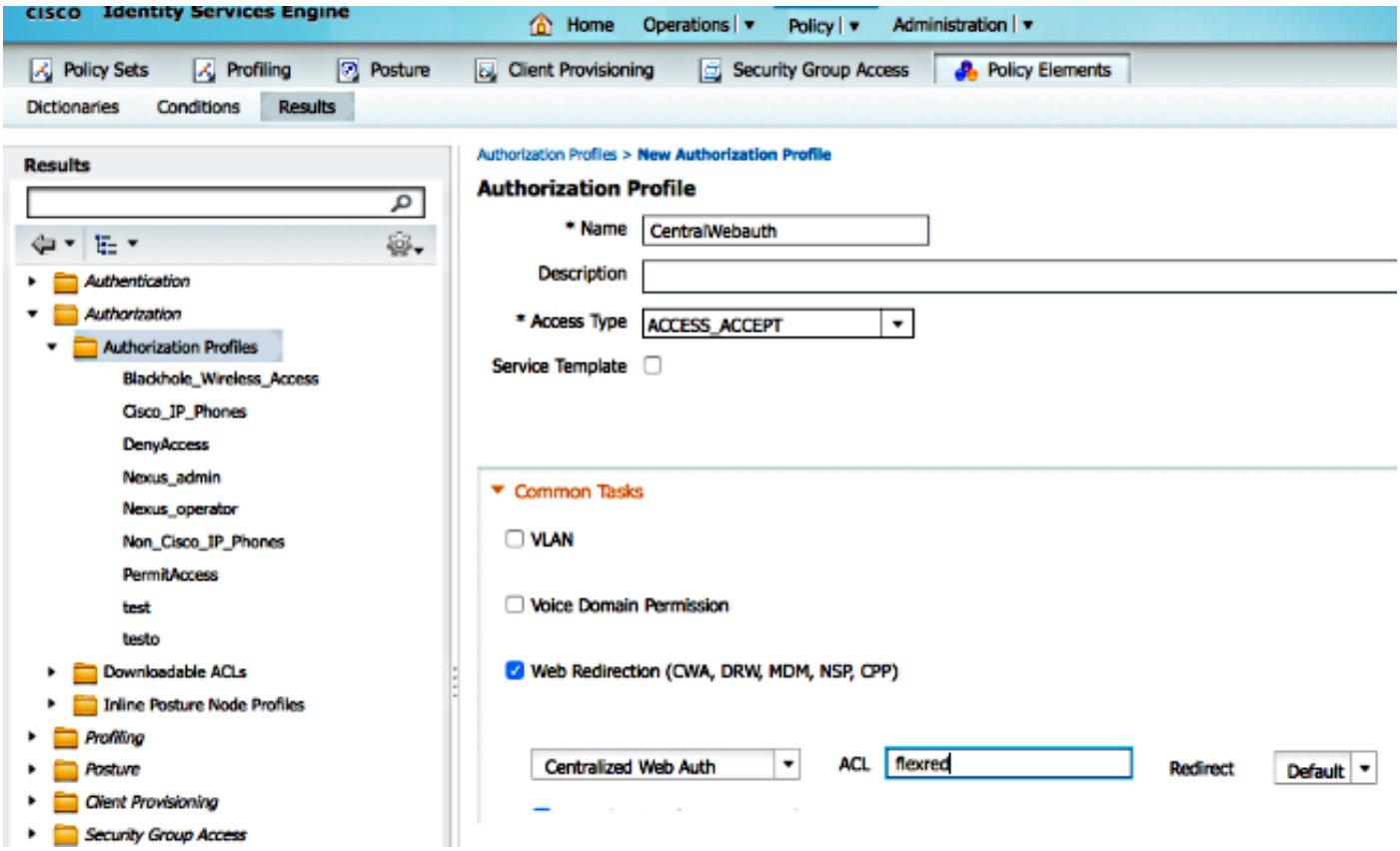
Gehen Sie wie folgt vor, um das Autorisierungsprofil zu erstellen:

1. Klicken Sie auf **Richtlinie** und dann auf **Richtlinienelemente**.
2. Klicken Sie auf **Ergebnisse**.
3. Erweitern Sie **Autorisierung**, und klicken Sie dann auf **Autorisierungsprofil**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**, um ein neues Autorisierungsprofil für die zentrale Webauthentifizierung zu erstellen.
5. Geben Sie im Feld **Name** einen Namen für das Profil ein. In diesem Beispiel wird *CentralWebauth* verwendet.
6. Wählen Sie **ACCESS_ACCEPT** aus der Dropdown-Liste "Access Type" aus.
7. Aktivieren Sie das Kontrollkästchen **Webauthentifizierung**, und wählen Sie **Zentrale Webauthentifizierung** aus der Dropdown-Liste aus.
8. Geben Sie im Feld ACL (ACL) den Namen der ACL auf dem WLC ein, die den

umzuleitenden Datenverkehr definiert. In diesem Beispiel wird *flexred* verwendet.

9. Wählen Sie in der Dropdown-Liste "Umleitung" die Option **Standard** aus.

Das Redirect-Attribut definiert, ob die ISE das Standard-Webportal oder ein vom ISE-Administrator erstelltes benutzerdefiniertes Webportal erkennt. In diesem Beispiel löst die *flexible* ACL eine Umleitung beim HTTP-Datenverkehr vom Client an einen beliebigen Standort aus.



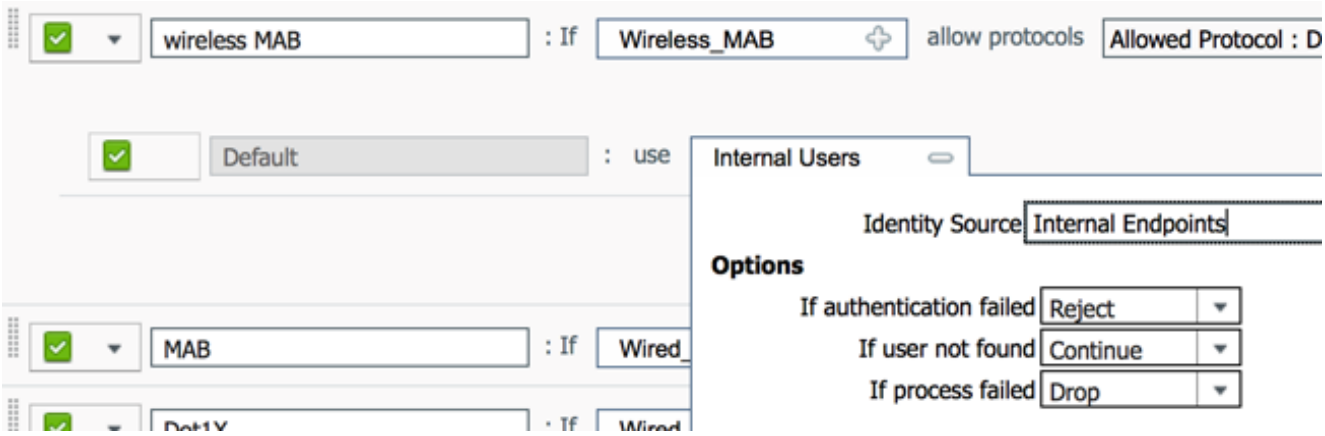
Erstellen einer Authentifizierungsregel

Führen Sie die folgenden Schritte aus, um die Authentifizierungsregel mithilfe des Authentifizierungsprofils zu erstellen:

1. Klicken Sie im Menü Richtlinie auf **Authentifizierung**. Dieses Bild zeigt ein Beispiel für die Konfiguration der Authentifizierungsrichtlinienregel. In diesem Beispiel wird eine Regel konfiguriert, die ausgelöst wird, wenn eine MAC-Filterung erkannt wird.

2. Geben Sie einen Namen für die Authentifizierungsregel ein. In diesem Beispiel wird *Wireless MAB* verwendet.
3. Wählen Sie das Plus-Symbol **(+)** im Feld If Bedingung.
4. Wählen Sie **Compound condition (Zusammengesetzte Bedingung)** und dann **Wireless_MAB (Wireless_MAB)**.

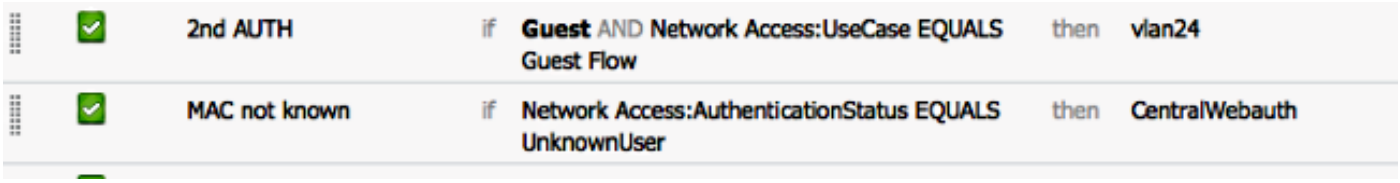
5. Wählen Sie "Standard-Netzwerkzugriff" als zulässiges Protokoll aus.
6. Klicken Sie auf den Pfeil neben **und ...**, um die Regel zu erweitern.
7. Klicken Sie im Feld Identity Source (Identitätsquelle) auf das Symbol **+**, und wählen Sie **Internal endpoints (Interne Endpunkte)**.
8. Wählen Sie in der Dropdown-Liste "Wenn Benutzer nicht gefunden" die Option **Weiter** aus.



Diese Option ermöglicht die Authentifizierung eines Geräts (über Webauth), auch wenn dessen MAC-Adresse nicht bekannt ist. Dot1x-Clients können sich weiterhin mit ihren Anmeldeinformationen authentifizieren und sollten von dieser Konfiguration nicht betroffen sein.

Erstellen einer Autorisierungsregel

In der Autorisierungsrichtlinie müssen nun mehrere Regeln konfiguriert werden. Wenn der PC zugeordnet ist, durchläuft er die MAC-Filterung. Es wird davon ausgegangen, dass die MAC-Adresse nicht bekannt ist, sodass die Webauth- und ACL-Adresse zurückgegeben werden. Diese *MAC*-Regel *ist* in der Abbildung unten dargestellt und in diesem Abschnitt konfiguriert.



Gehen Sie wie folgt vor, um die Autorisierungsregel zu erstellen:

1. Erstellen Sie eine neue Regel, und geben Sie einen Namen ein. In diesem Beispiel wird *MAC unbekannt* verwendet.
2. Klicken Sie auf das Plus-Symbol **(+)** im Bedingungsfeld, und wählen Sie eine neue Bedingung aus.
3. Erweitern Sie die Dropdownliste **Ausdruck**.
4. Wählen Sie **Netzwerkzugriff aus**, und erweitern Sie ihn.
5. Klicken Sie auf **AuthenticationStatus**, und wählen Sie den Operator **Equals aus**.
6. Wählen Sie im rechten Feld die Option **UnknownUser** aus.
7. Wählen Sie auf der Seite "General Authorization" (Allgemeine Autorisierung) **dann** im Feld rechts neben dem Wort "**Central Webauth**" (Autorisierungsprofil) aus.Mit diesem Schritt kann die ISE fortgesetzt werden, obwohl der Benutzer (oder die MAC-Adresse) nicht bekannt

ist.Unbekannte Benutzer werden nun mit der Anmeldeseite angezeigt. Nach Eingabe der Anmeldeinformationen wird ihnen jedoch erneut eine Authentifizierungsanforderung auf der ISE angezeigt. Daher muss eine andere Regel konfiguriert werden, die erfüllt ist, wenn es sich bei dem Benutzer um einen Gastbenutzer handelt. In diesem Beispiel wird *If UseridentityGroup equals Guest* verwendet, und es wird davon ausgegangen, dass alle Gäste dieser Gruppe angehören.

8. Klicken Sie auf die Aktionsschaltfläche am Ende der *MAC*-Regel *nicht bekannt*, und wählen Sie oben eine neue Regel aus.**Hinweis:** Es ist sehr wichtig, dass diese neue Regel vor der *MAC*-Regel *unbekannt* kommt.
9. Geben Sie im Namensfeld die **zweite AUTH** ein.
10. Wählen Sie eine Identitätsgruppe als Bedingung aus. In diesem Beispiel wurde **Guest** ausgewählt.

11. Klicken Sie im Bedingungsfeld auf das Plus-Symbol (**+**), und wählen Sie eine neue Bedingung aus.

12. Wählen Sie **Network Access aus**, und klicken Sie auf **UseCase**.

13. Wählen Sie **Equals** als Operator.

14. Wählen Sie **GuestFlow** als den richtigen Operanden aus. Das bedeutet, dass Sie nur dann Benutzer auffangen, die sich gerade auf der Webseite angemeldet haben und nach einer Autorisierungsänderung (der Gastfluss-Teil der Regel) wieder zurückkehren, wenn sie der Gast-Identitätsgruppe angehören.

15. Klicken Sie auf der Autorisierungsseite auf das Plus-(**+**)-Symbol (neben *diesem)*, um ein Ergebnis für Ihre Regel auszuwählen.

    In diesem Beispiel wird ein vorkonfiguriertes Profil (vlan34) zugewiesen; diese Konfiguration wird in diesem Dokument nicht dargestellt.

    Sie können eine Option **Zugriffsberechtigung** auswählen oder ein benutzerdefiniertes Profil erstellen, um das VLAN oder die gewünschten Attribute zurückzugeben.

Wichtiger Hinweis: In der ISE-Version 1.3 tritt der Anwendungsfall "Guest Flow" je nach Art der Webauthentifizierung möglicherweise nicht mehr auf. Die Autorisierungsregel müsste dann als einzig mögliche Bedingung die Gast-Benutzergruppe enthalten.

Aktivieren der IP-Verlängerung (optional)

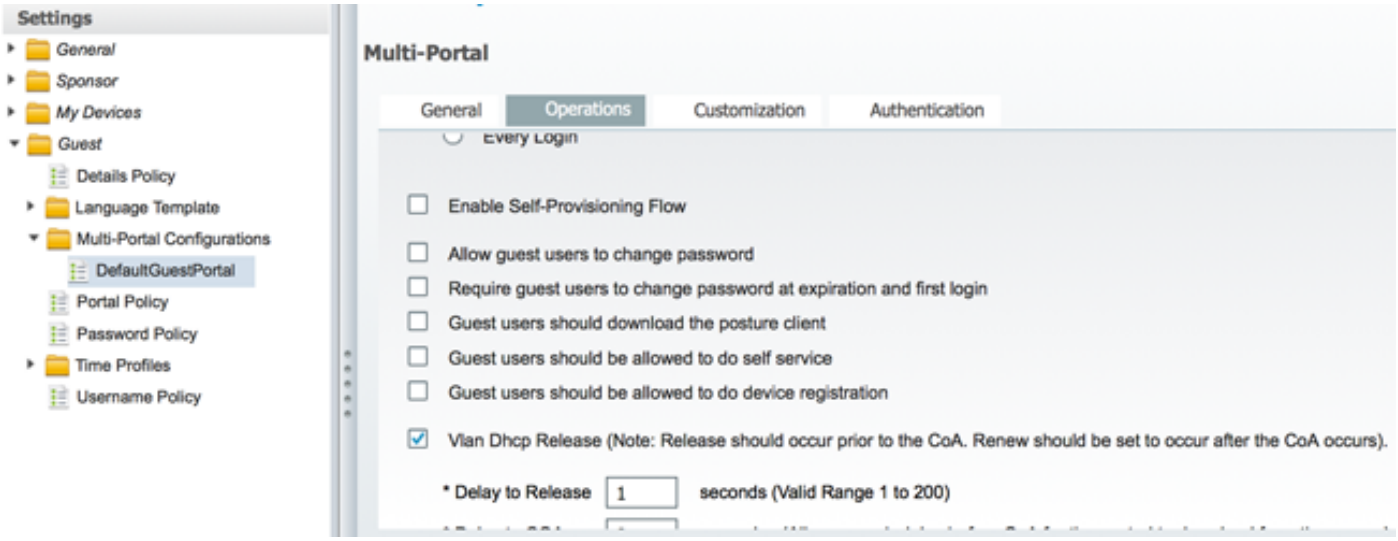
Wenn Sie ein VLAN zuweisen, besteht der letzte Schritt darin, dass der Client-PC seine IP-Adresse erneuert. Dieser Schritt wird durch das Gastportal für Windows-Clients erreicht. Wenn Sie kein VLAN für die *zweite AUTH*-Regel zuvor festgelegt haben, können Sie diesen Schritt überspringen.

Beachten Sie, dass das VLAN bei FlexConnect-APs bereits auf dem AP selbst vorhanden sein muss. Wenn dies nicht der Fall ist, können Sie eine VLAN-ACL-Zuordnung auf dem Access Point

selbst oder auf der Flex Group erstellen, bei der Sie keine ACL für das neue VLAN anwenden, das Sie erstellen möchten. Dadurch wird ein VLAN erstellt (ohne ACL).

Wenn Sie ein VLAN zugewiesen haben, führen Sie die folgenden Schritte aus, um die IP-Erneuerung zu aktivieren:

1. Klicken Sie auf **Administration** und dann auf **Guest Management**.
2. Klicken Sie auf **Einstellungen**.
3. Erweitern Sie **Gast**, und erweitern Sie dann **Multi-Portal Configuration**.
4. Klicken Sie auf **DefaultGuestPortal** oder den Namen eines benutzerdefinierten Portals, das Sie möglicherweise erstellt haben.
5. Klicken Sie auf das Kontrollkästchen **Vlan DHCP Release**.**Hinweis:** Diese Option funktioniert nur für Windows-Clients.



Datenverkehrsfluss

In diesem Szenario ist es schwierig zu verstehen, welcher Datenverkehr wohin gesendet wird. Hier eine kurze Zusammenfassung:

- Der Client sendet eine Zuordnungsanforderung per Funk für die SSID.
- Der WLC übernimmt die MAC-Filterauthentifizierung mit der ISE (wo er die Umleitungsattribute empfängt).
- Der Client erhält eine assoc-Antwort erst, nachdem die MAC-Filterung abgeschlossen ist.
- Der Client sendet eine DHCP-Anfrage, und zwar **LOKAL** durch den Access Point umgeschaltet, um eine IP-Adresse des dezentralen Standorts zu erhalten.
- Im Status "Central_webauth" ist der Datenverkehr, der in der Umleitungs-ACL als "Denial" markiert ist (normalerweise HTTP), **ZENTRAL** Switched. Die Umleitung übernimmt also nicht der WAP, sondern der WLC. Wenn der Client beispielsweise nach einer Website fragt, sendet der WAP diese an den CAPWAP-gekapselten WLC, und der WLC spiegelt diese Website-IP-Adresse vor und leitet sie zur ISE um.
- Der Client wird an die ISE-Umleitungs-URL umgeleitet. Dies ist **LOKAL** wieder eingeschaltet (weil er auf "Zulassen" auf der Flexredirect-ACL trifft).
- Sobald der Datenverkehr im Status "RUN" ist, wird er lokal geswitcht.

Überprüfung

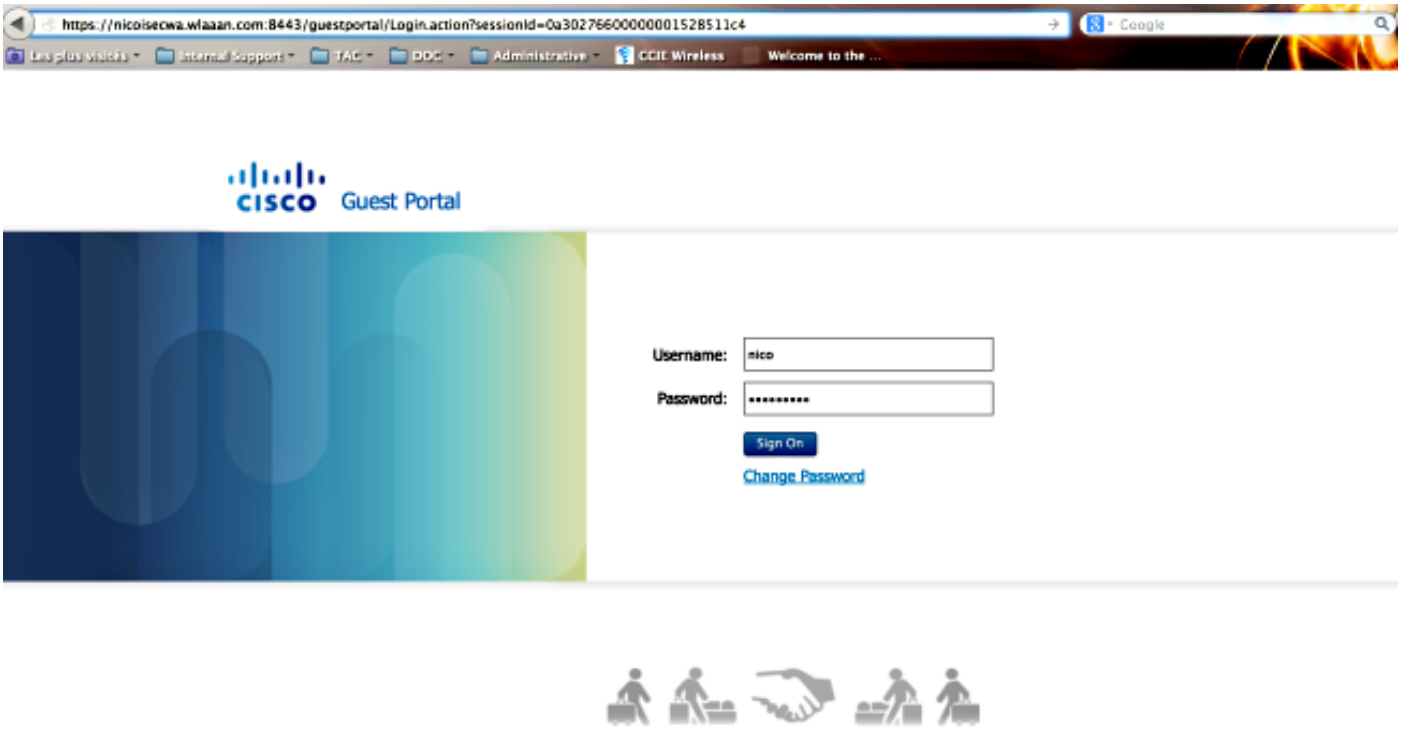
Sobald der Benutzer mit der SSID verknüpft ist, wird die Autorisierung auf der ISE-Seite

angezeigt.

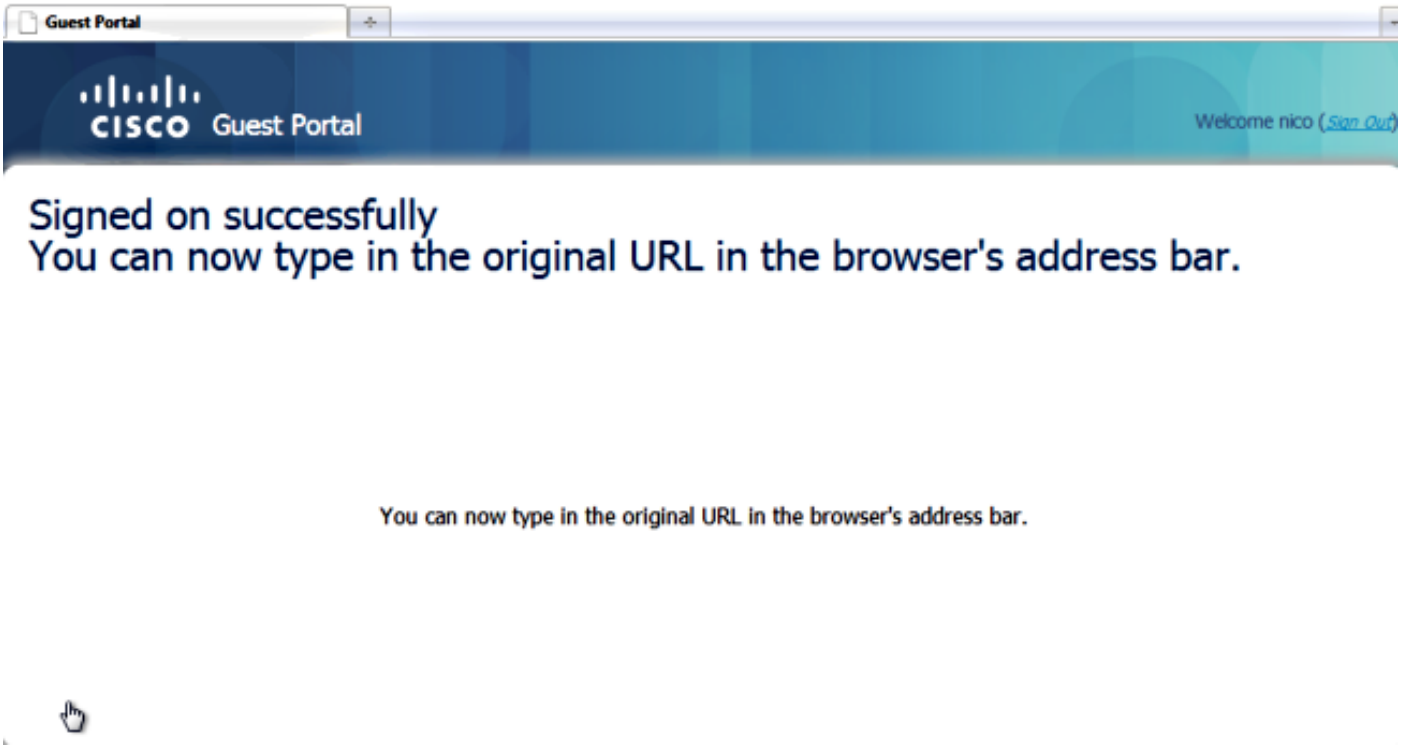
Apr 09,13 11:49:27.179 AM	✓		Nico	00:13:10:21:70:13	nicowlc	vlan34	Guest	NotApplicable	
Apr 09,13 11:49:27.174 AM	✓				nicowlc				Dynamic Author...
Apr 09,13 11:48:58.372 AM	✓		Nico	00:13:10:21:70:13			Guest		Guest Authentic..
Apr 09,13 11:47:19.475 AM	✓		00:13:10:21:70:13	00:13:10:21:70:13	nicowlc	CentralWebauth		Pending	Authentication ...

Von unten nach oben sehen Sie die Authentifizierung durch MAC-Adressfilterung, die die CWA-Attribute zurückgibt. Als Nächstes sehen Sie die Portal-Anmeldung mit dem Benutzernamen. Die ISE sendet dann eine CoA an den WLC, und die letzte Authentifizierung ist eine Layer-2-MAC-Filterauthentifizierung auf der WLC-Seite. Die ISE erinnert sich jedoch an den Client und den Benutzernamen und wendet das in diesem Beispiel konfigurierte VLAN an.

Wenn eine beliebige Adresse auf dem Client geöffnet wird, wird der Browser zur ISE umgeleitet. Stellen Sie sicher, dass das Domain Name System (DNS) richtig konfiguriert ist.



Der Netzwerkzugriff wird gewährt, nachdem der Benutzer die Richtlinien akzeptiert hat.



Auf dem Controller werden der Status des Richtlinien-Managers und der RADIUS NAC-Status von *POSTURE_REQD* in *RUN* geändert.

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.