Konfigurieren der externen Webauthentifizierung mit konvergentem Zugriff (5760/3650/3850)

Inhalt

Einführung

In diesem Dokument wird die Konfiguration einer externen Webauthentifizierung mit konvergenten Zugriffs-Controllern erläutert. Die Seite des Gastportals und die Authentifizierung der Anmeldeinformationen finden sich in diesem Beispiel sowohl auf Identity Services Engine (ISE).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

1. Cisco Converged Access Controller.

2. Webauthentifizierung

3. Cisco ISE

Verwendete Komponenten

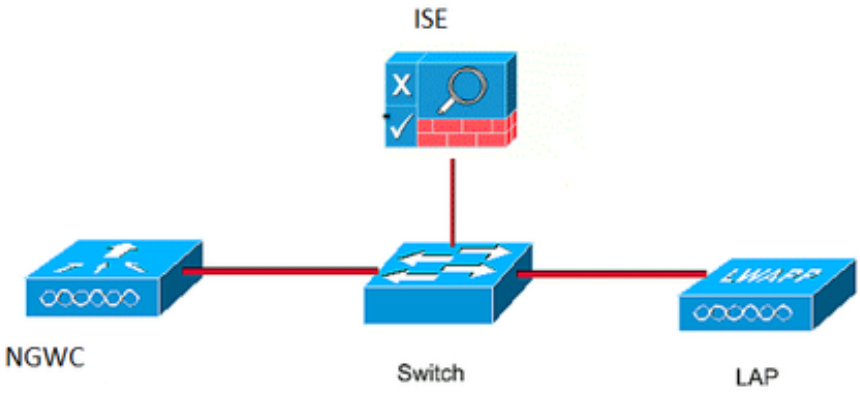
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

1. Cisco 5760 Controller (NGWC im folgenden Diagramm), 03.06.05E

2. ISE 2.2

Konfigurieren

Netzwerkdiagramm



CLI-Konfiguration

Radius-Konfiguration für Controller

Schritt 1: Definieren des externen Radius-Servers

```
radius server ISE.161
address ipv4 10.48.39.161 auth-port 1812 acct-port 1813
timeout 10
retransmit 5
key Cisco123
```

Schritt 2:. Definieren der AAA-Radius-Gruppe und Angeben des zu verwendenden Radius-Servers

```
aaa group server radius ISE-Group
server name ISE.161
deadtime 10
```

Schritt 3. Definieren Sie eine Methodenliste, die auf die Radius-Gruppe verweist, und ordnen Sie sie unter dem WLAN zu.

```
aaa authentication login webauth group ISE-Group
```

Konfiguration der Parameterzuordnung

Schritt 4. Konfigurieren Sie die globale Parameterzuordnung mit der virtuellen IP-Adresse, die für die externe und interne Webauth erforderlich ist. Die Abmeldungstaste verwendet die virtuelle IP. Es empfiehlt sich immer, eine nicht routbare virtuelle IP zu konfigurieren.

```
parameter-map type webauth global
type webauth
virtual-ip ipv4 1.1.1.1
```

Schritt 5: Konfigurieren Sie eine benannte Parameterzuordnung. Sie funktioniert wie ein Typ von Webauth-Methode. Diese wird unter der WLAN-Konfiguration aufgerufen.

```
parameter-map type webauth web
type webauth
redirect for-login https://10.48.39.161:8443/portal/PortalSetup.action?portal=0c712cd0-6d90-
11e5-978e-005056bf2f0a
redirect portal ipv4 10.48.39.161
```

ACL vor der Authentifizierung. Dies wird auch unter dem WLAN aufgerufen.

Schritt 6: Konfigurieren Sie Preauth_ACL, die den Zugriff auf ISE, DHCP und DNS ermöglicht, bevor die Authentifizierung vorüber ist.

```
ip access-list extended Preauth_ACL
permit ip any host 10.48.39.161
permit ip host 10.48.39.161 any
permit udp any eq bootps any
permit udp any any eq bootpc
permit udp any eq bootpc any
permit udp any eq domain any
permit udp any any eq domain
```

WLAN-Konfiguration

Schritt 7: WLAN konfigurieren

```
wlan ext-webauth 7 ext-webauth
client vlan vlan232
ip access-group web Preauth_ACL
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list webauth
security web-auth parameter-map web
session-timeout 1800
no shutdown
```

Schritt 8: Aktivieren Sie den HTTP-Server.

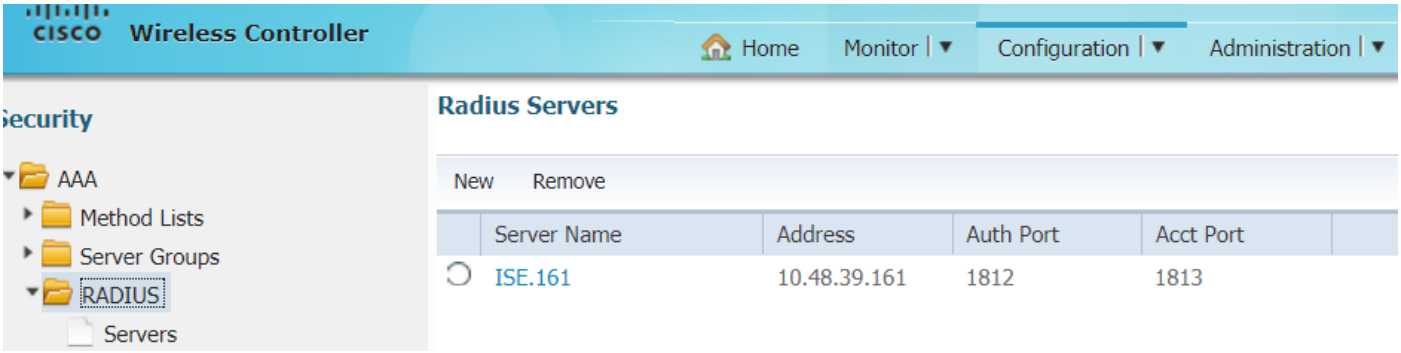
```
ip http server

ip http secure-server (for secure web-auth, use 'no' to disable secure web)
```

GUI-Konfiguration

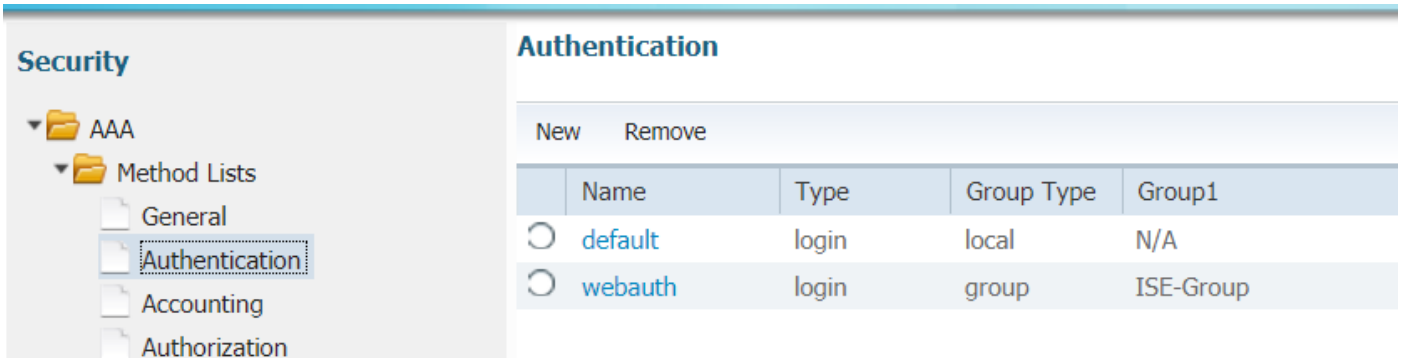
Wir befolgen hier dieselben Schritte wie oben. Die Screenshots dienen lediglich als Querverweis.

Schritt 1: Definieren eines externen Radius-Servers



Schritt 2:. Definieren der AAA-Radius-Gruppe und Angeben des zu verwendenden Radius-Servers

Schritt 3. Definieren Sie eine Methodenliste, die auf die Radius-Gruppe verweist, und ordnen Sie sie unter dem WLAN zu.



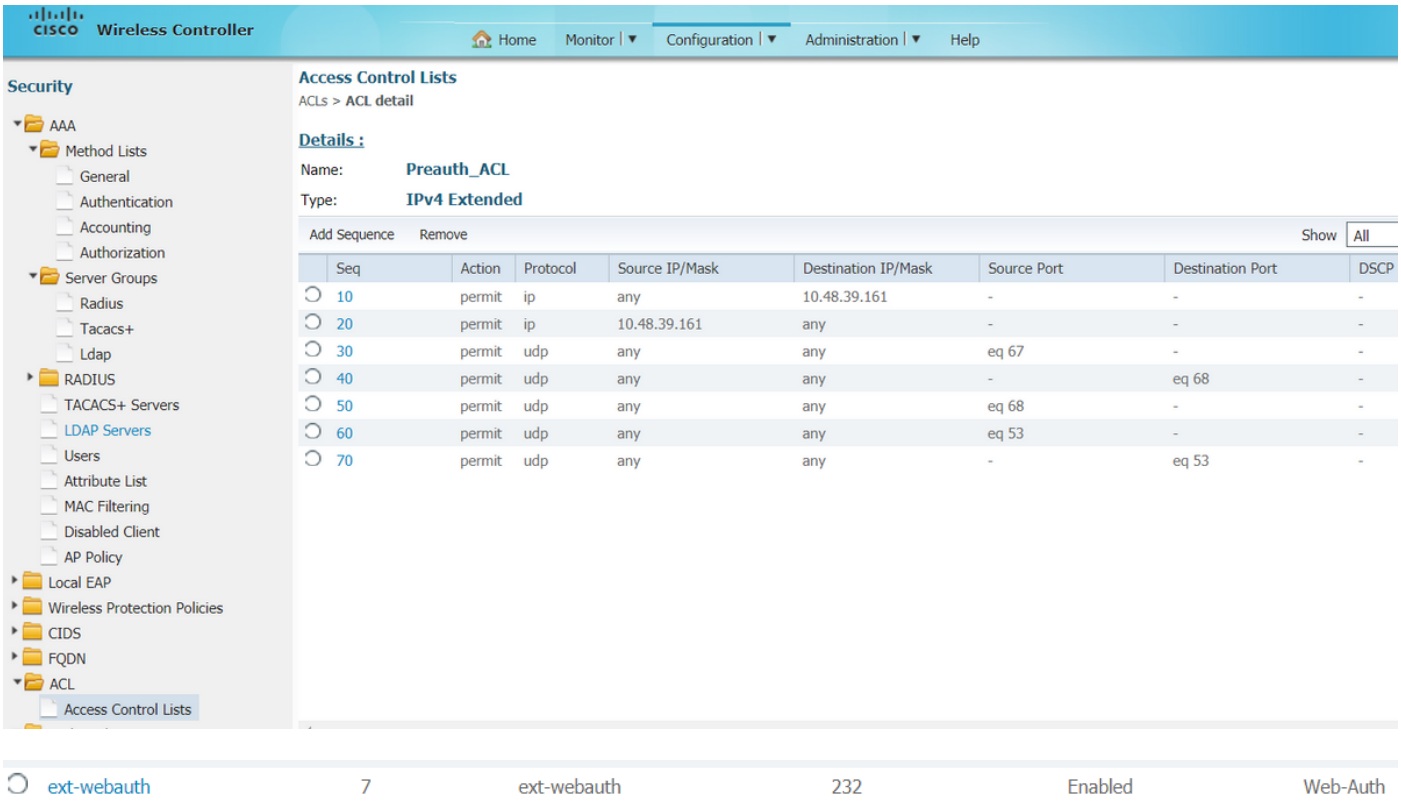
Konfiguration der Parameterzuordnung

Schritt 4. Konfigurieren Sie die globale Parameterzuordnung mit der virtuellen IP-Adresse, die für die externe und interne Webauth erforderlich ist. Die Abmeldungstaste verwendet die virtuelle IP. Es empfiehlt sich immer, eine nicht routbare virtuelle IP zu konfigurieren.

Schritt 5: Konfigurieren Sie eine benannte Parameterzuordnung. Sie funktioniert wie ein Typ von Webauth-Methode. Diese wird unter der WLAN-Konfiguration aufgerufen.

ACL vor der Authentifizierung. Dies wird auch unter dem WLAN aufgerufen.

Schritt 6: Konfigurieren Sie Preauth_ACL, die den Zugriff auf ISE, DHCP und DNS ermöglicht, bevor die Authentifizierung vorüber ist.

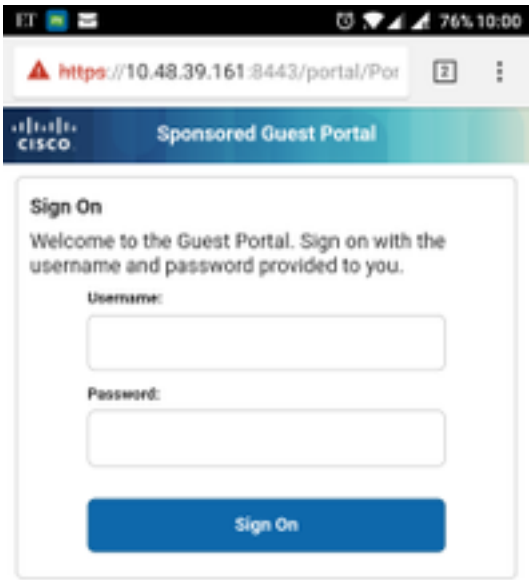


WLAN-Konfiguration

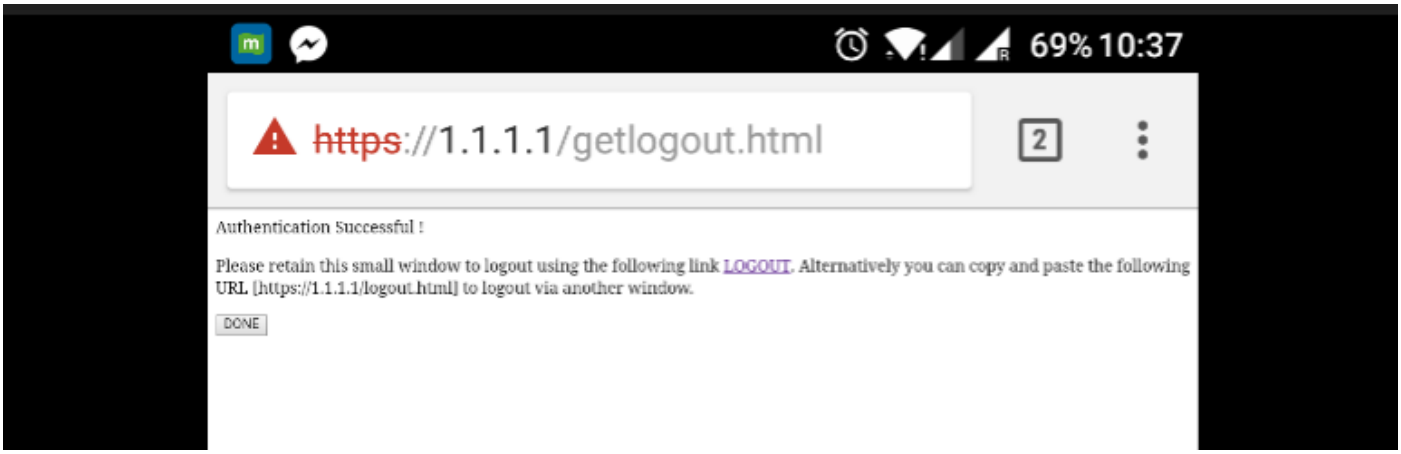
Schritt 7: WLAN konfigurieren

Überprüfen

Schließen Sie einen Client an, und stellen Sie sicher, dass der Client beim Öffnen eines Browsers auf Ihre Login-Portal-Seite umgeleitet wird. Der folgende Screenshot zeigt die Seite für das ISE-Gastportal.



Wenn die richtigen Anmeldeinformationen übermittelt wurden, wird die Erfolgsseite angezeigt:



Der ISE-Server meldet zwei Authentifizierungen: eine auf der Gast-Seite selbst (die untere Zeile nur mit dem Benutzernamen) und eine zweite Authentifizierung, sobald der WLC den gleichen Benutzernamen/das gleiche Kennwort durch RADIUS-Authentifizierung bereitstellt (nur diese Authentifizierung führt dazu, dass der Client in die Erfolgsphase wechselt). Wenn die RADIUS-Authentifizierung (mit MAC-Adresse und WLC-Details als NAS) nicht erfolgt, ist die Radius-Konfiguration zu überprüfen.