

Externe webverificatie met geconvergeerde access point (5760/3650/3850) configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[CLI-configuratie](#)

[GUI-configuratie](#)

[Verifiëren](#)

Inleiding

Dit document definieert hoe u externe webauth kunt configureren met geconvergeerde toegangscontrollers. De website van het gastportaal en de authenticatie van geloofsbrieven zijn zowel op Identity Services Engine (ISE) in dit voorbeeld.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

1. Cisco geconvergeerde toegangscontrollers
2. Web-verificatie
3. Cisco ISE

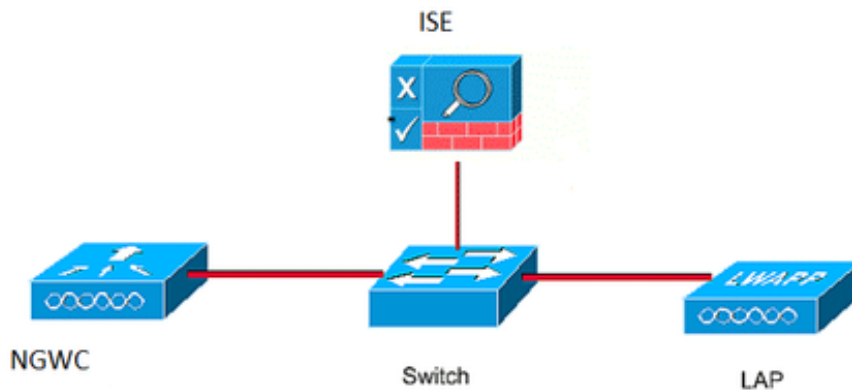
Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

1. Cisco 5760 controller (NGWC op het onderstaande schema), 3.06.05E
2. ISE 2.2

Configureren

Netwerkdigram



CLI-configuratie

Straal configuratie van de controller

stap 1 : Afzonderlijke Straalserver definiëren

```

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

stap 2: Definieer AAA Straalgroep en specificeer de te gebruiken Straalserver

```

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

Stap 3. Stel een methodelijst op die naar de pijltjesgroep is gericht en stel deze in onder het WLAN.

```

aaa authentication login webauth group ISE-Group
  
```

Configuratie parameter-kaart

stap 4. Configuratie van de globale parameter kaart met virtueel ip adres dat nodig is voor de externe en interne website. De knop Uitloggen gebruikt virtuele IP. Het is altijd een goede praktijk om een niet routeerbare virtuele ip te configureren.

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

stap 5 : Configureer een parameter map. Deze werkt als een soort webauth-methode. Dit zal worden opgeroepen onder de WLAN-configuratie.

```
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
```

Verificatie vooraf. Dit zal ook worden opgeroepen onder het WLAN.

stap 6 : Configureer Preauth_ACL waardoor toegang tot ISE, DHCP en DNS mogelijk is voordat de verificatie is verlopen

```
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-configuratie

stap 7 : configureren: WLAN

```
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
```

stap 8 : Zet de http server aan.

```
ip http server
```

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

GUI-configuratie

Wij volgen hier dezelfde stappen als hierboven. De screenshots worden zojuist geplaatst voor referentie.

stap 1 : Een externe straal-server definiëren

CISCO Wireless Controller

Home Monitor Configuration Administration

Security

- AAA
 - Method Lists
 - Server Groups
 - RADIUS**
 - Servers

Radius Servers

New Remove

	Server Name	Address	Auth Port	Acct Port
<input type="radio"/>	ISE.161	10.48.39.161	1812	1813

stap 2: Definieer AAA Straalgroep en specificeer de te gebruiken Straalserver

Security

- AAA
 - Method Lists
 - Server Groups
 - Radius**
 - Tacacs

Radius Server Groups

New Remove

	Name	Server1
<input type="radio"/>	ISE-Group	ISE.161

Stap 3. Stel een methodelijst op die naar de pijltjesgroep is gericht en stel deze in onder het WLAN.

Security

- AAA
 - Method Lists
 - General
 - Authentication**
 - Accounting
 - Authorization

Authentication

New Remove

	Name	Type	Group Type	Group1
<input type="radio"/>	default	login	local	N/A
<input type="radio"/>	webauth	login	group	ISE-Group

Configuratie parameter-kaart

stap 4. Configuratie van de globale parameter kaart met virtueel ip adres dat nodig is voor de externe en interne website. De knop Uitloggen gebruikt virtuele IP. Het is altijd een goede praktijk om een niet routeerbare virtuele ip te configureren.

stap 5 : Configureer een parameter map. Deze werkt als een soort webauth-methode. Dit zal worden opgeroepen onder de WLAN-configuratie.

CISCO Wireless Controller

Home Monitor Configuration Administration

Security

- AAA
 - Method Lists
 - General
 - Authentication
 - Accounting
 - Authorization

Webauth Parameter Map

New Remove

	Parameter-map name	Parameter-map type
<input type="radio"/>	global	Global
<input type="radio"/>	web	Named

Verificatie vooraf. Dit zal ook worden opgeroepen onder het WLAN.

stap 6 : Configureer Preauth_ACL waardoor toegang tot ISE, DHCP en DNS mogelijk is voordat de verificatie is verlopen

The screenshot shows the Cisco Wireless Controller interface. The left sidebar is under 'Security' > 'ACL' > 'Access Control Lists'. The main area is titled 'Access Control Lists' and shows details for 'Preauth_ACL' (Type: IPv4 Extended). A table lists the ACL entries:

Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port	DSCP
10	permit	ip	any	10.48.39.161	-	-	-
20	permit	ip	10.48.39.161	any	-	-	-
30	permit	udp	any	any	eq 67	-	-
40	permit	udp	any	any	-	eq 68	-
50	permit	udp	any	any	eq 68	-	-
60	permit	udp	any	any	eq 53	-	-
70	permit	udp	any	any	-	eq 53	-

ext-webauth	7	ext-webauth	232	Enabled	Web-Auth
-------------	---	-------------	-----	---------	----------

WLAN-configuratie

stap 7 : configureren: WLAN

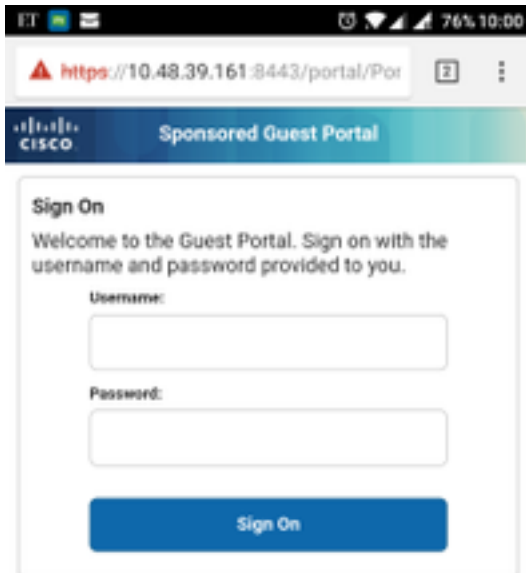
The screenshot shows the Cisco Wireless Controller interface for WLAN configuration. The left sidebar is under 'Wireless' > 'WLAN' > 'WLANs'. The main area is titled 'WLAN' and shows the 'Edit' configuration for a WLAN. The 'Security' tab is selected, and the 'Layer3' tab is active. The configuration includes:

- Web Policy:
- Conditional Web Redirect:
- Webauth Authentication List: webauth
- Webauth Parameter Map: web
- Webauth On-mac-filter Failure:
- Preauthentication IPv4 ACL: Preauth_ACL
- Preauthentication IPv6 ACL: none

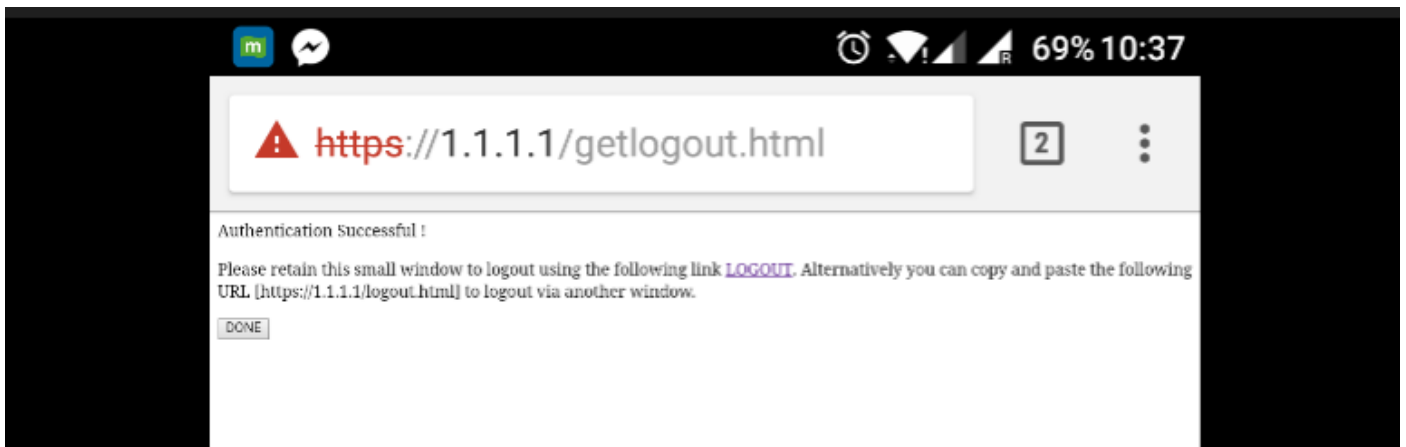
Verifiëren

Sluit een client aan en controleer of als u een browser opent, de client opnieuw wordt gericht naar de pagina met uw inlogportal. Onderstaande screenshot illustreert de pagina van het ISE-

gastartaal.



Zodra er voldoende aanmeldingsgegevens zijn ingediend, wordt de succespagina weergegeven:



De ISE server zal twee authenticatie melden : één op de gastpagina zelf (de onderste lijn met alleen de gebruikersnaam) en een tweede authenticatie zodra de WLC dezelfde gebruikersnaam/wachtwoord door middel van strafinthectie verstrekt (alleen deze authenticatie zal de client naar de succesfase verhuizen). Als de detectie van de straal (met hoofdadres en WLC-gegevens als NAS) niet optreedt, moet de configuratie van de straal worden geverifieerd.

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...
Sep 10, 2017 08:37:37.891 AM	✓			ritmahaj	C0:EE:FB:D7:88:24	Unknown	Default >> D...	Default >> B...	PermitAccess
Sep 10, 2017 08:37:34.506 AM	✓			ritmahaj					