

Configureer ISE draadloze WAN- en hotspotstromen met AireOS en WLC's van de volgende generatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Unified 5508 WLC configureren](#)

[Wereldwijde configuratie](#)

[Configureer de Service Set Identifier \(SSID\) van de gast:](#)

[Configureer de omleiding van de ACL](#)

[HTTPS-omleiding](#)

[Agressieve failover](#)

[Omlleiding voor intern gebruik](#)

[Configureer geconvergeerde 3850 NGWC](#)

[Wereldwijde configuratie](#)

[SSID-configuratie](#)

[Configuratie ACL-omleiding](#)

[CLI-configuratie \(Command-Line Interface\)](#)

[ISE configureren](#)

[Gemeenschappelijke ISE-configuratietaken](#)

[Use case 1: CWA met gastverificatie in elke gebruikersverbinding](#)

[Use case 2: CWA met apparaatregistratie die de gastenverificatie eenmaal per dag uitvoert.](#)

[Use case 3: hostspotportal](#)

[Verifiëren](#)

[Use Case 1](#)

[Use Case 2](#)

[Use Case 3](#)

[FlexConnect lokale switching in AireOS](#)

[buitenlands ankerscenario](#)

[Problemen oplossen](#)

[Veelvoorkomende verbroken statussen op zowel AireOS als geconvergeerde access WLC](#)

[AireOS WLC](#)

[NGWC](#)

[ISE](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u drie gastcases kunt configureren in de Identity Services Engine met Cisco AireOS- en Next Generation Wireless LAN-controllers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco draadloze LAN-controllers (Unified en geconvergeerde toegang)
- Identity Services Engine (ISE)

Gebruikte componenten

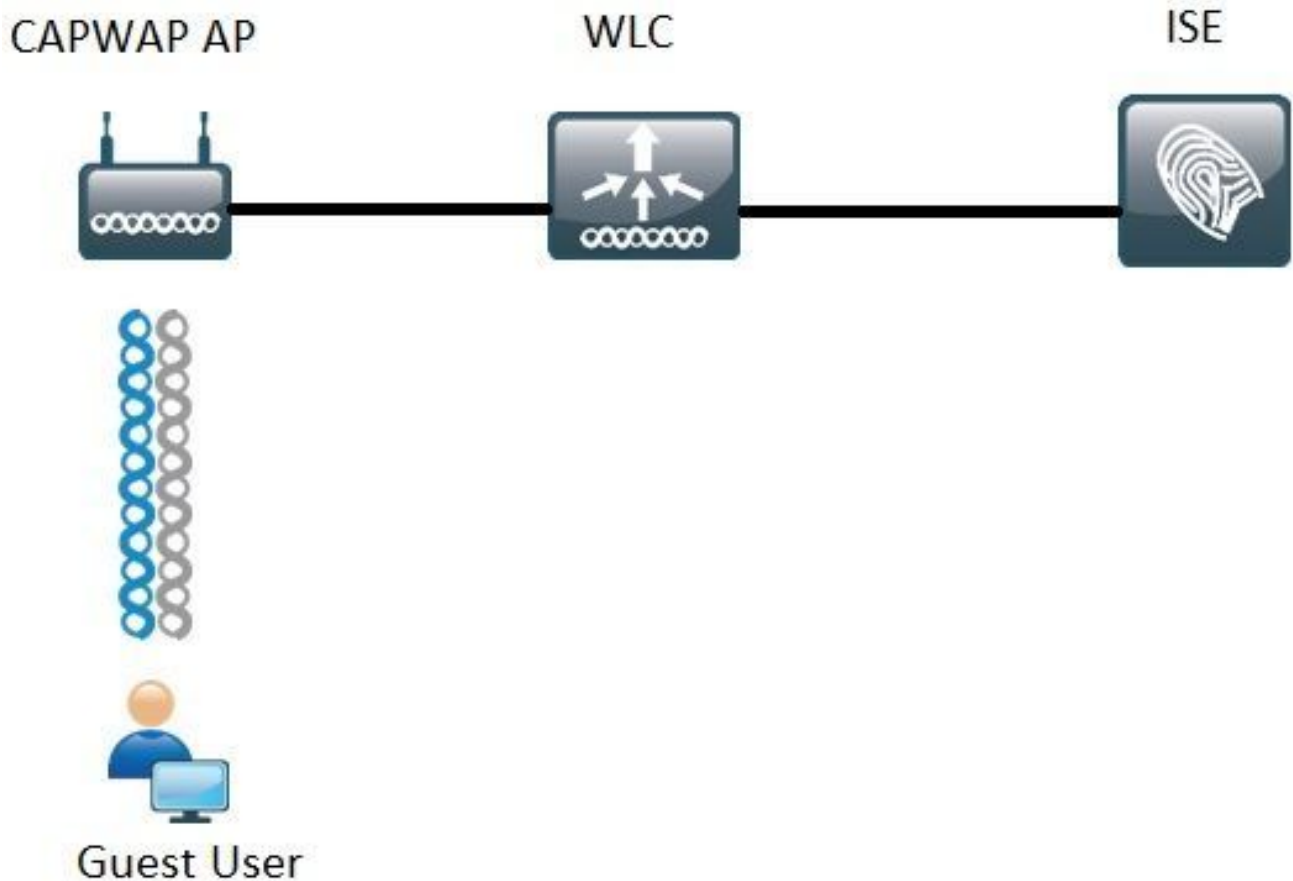
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine versie 2.1
- Cisco draadloze LAN-controller 5508 met 8.0.121.0
- Catalyst 3850 (WS-C3850-24P) met draadloze controller van de volgende generatie (NGWC) en 03.06.04.E

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdigram



De stappen die in dit document worden behandeld beschrijven de typische configuratie op zowel Unified als Converged Access WLC's om het even welke Gaststroom met ISE te steunen.

Unified 5508 WLC configureren

Ongeacht de gebruikscase die in ISE is geconfigureerd, vanuit het WLC-perspectief begint alles met een draadloos eindpunt dat verbinding maakt met een Open SSID met MAC-filtering ingeschakeld (Plus AAA-overschrijving en RADIUS NAC) die naar ISE wijst als de verificatie- en accountingserver. Dit zorgt ervoor dat ISE dynamisch de nodige attributen aan WLC kan duwen voor een succesvolle handhaving van een redirect naar ISE's Guest Portal.

Wereldwijde configuratie

1. Voeg ISE wereldwijd toe als een verificatie- en accounting server.
 - Navigeer naar **Beveiliging > AAA > Verificatie** en klik op **Nieuw**



- Voer IP van ISE-server en gedeeld geheim in
- Zorg ervoor dat de serverstatus en de **ondersteuning voor RFC 3676** (wijziging van autorisatie of CoA-ondersteuning) beide zijn ingesteld op **Ingeschakeld**.
- Onder server timeout door standaard AireOS WLCs heeft 2 seconden. Door op de netwerkenmerken (latency, ISE en WLC op verschillende locaties) te scharnieren, kan het voordelig zijn om de time-out van de server te verhogen tot ten minste 5 seconden om onnodige failover-gebeurtenissen te voorkomen.
- Klik op **Apply** (Toepassen).
- Als er meerdere Policy Services Nodes (PSN) zijn om te configureren, gaat u verder om extra serververmeldingen aan te maken.

Opmerking: dit specifieke configuratievoorbeeld bevat 2 ISE-exemplaren

- Navigeer naar **Security > AAA > RADIUS > Accounting** en klik op **Nieuw**
- Voer IP van ISE-server en gedeeld geheim in
- Zorg ervoor dat de serverstatus is ingesteld op Ingeschakeld
- Verhoog indien nodig de server timeout (standaard is 2 seconden).

2. Fallback-configuratie.

In een eengemaakte omgeving, zodra de server timeout wordt geactiveerd, gaat WLC naar de volgende geconfigureerde server. Volgende in lijn van WLAN. Als er geen andere beschikbaar is, selecteert de WLC de volgende in de globale serverlijst. Wanneer meerdere servers zijn geconfigureerd op de SSID (Primair, Secundair) zodra de failover optreedt, blijft de WLC standaard verificatie en (of) accounting verkeer permanent naar de Secundaire instantie sturen, zelfs als de primaire server weer online is.

Om dit gedrag te verzachten, maak je fallback mogelijk. Navigeer naar **Security > AAA > RADIUS > Fallback**. Het standaardgedrag is uit. De enige manier om van een server-down gebeurtenis te herstellen vereist admin interventie (globaal stuiten de admin status van de server).

Om reserve in te schakelen hebt u twee opties:

- **Passief** - In passieve modus, als een server niet reageert op het WLC-verificatieverzoek,

verplaatst de WLC de server naar inactieve wachtrij en stelt een timer in (Interval in Sec-optie). Wanneer de timer verloopt, verplaatst de WLC de server naar actieve wachtrij ongeacht de feitelijke status van de servers. Als het verificatieverzoek resulteert in een timeout-gebeurtenis (wat betekent dat de server nog steeds niet actief is), wordt de serverinvoer opnieuw verplaatst naar de inactieve wachtrij en wordt de timer opnieuw ingeschakeld. Als de server met succes terugantwoordt, blijft het in de Actieve rij. Configureerbare waarden gaan hier van 180 tot 3600 seconden.

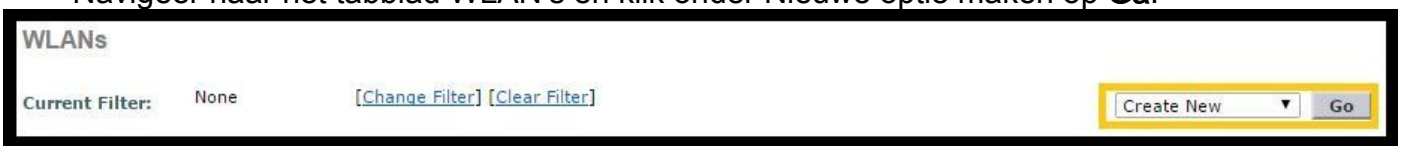
- **Actief** - In actieve modus, wanneer een server niet reageert op het WLC-verificatieverzoek, merkt de WLC de server als dood, verplaatst de server naar niet-actieve serverpool en begint periodiek sonde-berichten te verzenden totdat die server reageert. Als de server reageert, dan verplaatst de WLC de dode server naar de actieve pool en stopt het verzenden van sonde berichten.

In deze modus vereist de WLC dat u in seconden (180 tot 3600) een gebruikersnaam en een sonde-interval invoert.

Opmerking: WLC-sonde vereist geen succesvolle verificatie. Hoe dan ook, een succesvolle of mislukte verificatie wordt beschouwd als een serverrespons die voldoende is om de server naar de actieve wachtrij te promoten.

Configureer de Service Set Identifier (SSID) van de gast:

- Navigeer naar het tabblad WLAN's en klik onder Nieuwe optie maken op **Ga**:



- Voer een profielnaam en een SSID-naam in. Klik op **Apply** (Toepassen).
- Selecteer onder het tabblad General de interface of de interfacegroep die gebruikt moet worden (Guest VLAN).



- Onder **Security > Layer 2 > Layer 2 Security** selecteert u **Geen** en schakelt u het selectievakje voor **Mac-filtering** in.



- Stel onder het tabblad **AAA-servers** verificatie- en accounting-servers in op **ingeschakeld** en selecteer uw primaire en secundaire servers.



- **Tussentijdse update:** Dit is een optionele configuratie die geen voordelen aan deze stroom toevoegt. Als u het liever inschakelt, moet de WLC 8.x of hogere code uitvoeren:

Uitgeschakeld: de functie is volledig uitgeschakeld.

Ingeschakeld met 0 Interval: De WLC stuurt boekhoudkundige updates naar ISE telkens als er een wijziging is in de MSCB-ingang (Mobile Station Control Block) van de client. IPv4- of IPv6-adrestoewijzing of -wijziging, client roaming-event.) Er worden geen extra periodieke updates verzonden.

Ingeschakeld met een ingesteld Interim Interval: In deze modus stuurt de WLC meldingen naar ISE op de MSCB-ingangswijzigingen van de client en stuurt ze ook extra periodieke boekhoudmeldingen met het ingestelde interval (ongeacht eventuele wijzigingen).

- Selecteer onder het tabblad **Advanced** de optie **AAA negeren toestaan** en selecteer onder **NAC-status RADIUS NAC**. Dit zorgt ervoor dat WLC om het even welke attributenwaardeparen (AVPs) toepast die van ISE komen.
- Navigeer naar het algemene tabblad **SSID** en stel de status van de SSID in op **Ingeschakeld**

WLANs > Edit 'Guest'

The screenshot shows the configuration page for a WLAN named 'Guest'. The 'Advanced' tab is selected. The 'Status' is set to 'Enabled' with a checked checkbox. Other fields like Profile Name, Type, and SSID are also visible.

- Pas de wijzigingen toe.

Configureer de omleiding van de ACL

Deze ACL wordt van verwijzingen voorzien door ISE en bepaalt welk verkeer wordt omgeleid en welk verkeer door wordt toegestaan.

- Ga naar het tabblad **Beveiliging > Toegangscontrolelijsten** en klik op **Nieuw**
- Dit is een voorbeeld van ACL

The screenshot shows the 'Access Control Lists > Edit' page for 'Guest_Redirect'. It displays a table of ACL rules with columns for Seq, Action, Source IP/Mask, Destination IP/Mask, Protocol, Source Port, Dest Port, DSCP, Direction, and Number of Hits.

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Any	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	DNS	Any	Any	Any	0
3	Permit	0.0.0.0 / 0.0.0.0	157.210 / 255.255.255.255	TCP	Any	8443	Any	Any	0
4	Permit	157.210 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0
5	Permit	0.0.0.0 / 0.0.0.0	157.21 / 255.255.255.255	TCP	Any	8443	Any	Any	0
6	Permit	157.21 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8443	Any	Any	Any	0

Deze ACL moet toegang verlenen tot en van DNS-services en ISE-knooppunten via TCP-poort 8443. Er is een impliciete ontkenning onderaan dat betekent de rest van het verkeer wordt omgeleid naar ISE's Guest Portal URL.

HTTPS-omleiding

Deze optie wordt ondersteund in AireOS-versies 8.0.x en hoger, maar wordt standaard uitgeschakeld. Als u HTTPS-ondersteuning wilt inschakelen, gaat u naar **WLC Management > HTTP-HTTPS > HTTPS-omleiding** en stelt u deze optie in op **Ingeschakeld** of past u deze opdracht toe in CLI:


```
(Cisco Controller) >config network web-auth https-redirect enable
```

Waarschuwingen certificaat nadat HTTPS-omleiding is ingeschakeld

Nadat https-redirect is ingeschakeld, kan de gebruiker tijdens de redirect problemen met het certificaat vertrouwen ervaren. Dit wordt zelfs gezien als er een geldig kettingcertificaat op de controller is en zelfs als dit certificaat is ondertekend door een vertrouwde certificeringsinstantie van een derde partij. De reden is dat het certificaat dat op de WLC is geïnstalleerd, wordt afgegeven aan de virtuele interface hostname of IP-adres. Wanneer de client https probeert://cisco.com, verwacht de browser dat het certificaat wordt afgegeven aan cisco.com. Echter, om de WLC in staat te stellen de GET afgegeven door de client te onderscheppen, moet het eerst de HTTPS sessie instellen waarvoor de WLC zijn Virtual Interface Certificate presenteert tijdens SSL handshake fase. Dit zorgt ervoor dat de browser een waarschuwing weergeeft, aangezien het certificaat dat tijdens de SSL-handdruk wordt gepresenteerd, niet is afgegeven aan de oorspronkelijke website die de client probeert te bereiken (dat wil zeggen: cisco.com tegen WLC's Virtual interface hostname). U kunt verschillende certificaat foutmeldingen in verschillende browsers zien, maar alle hebben betrekking op hetzelfde probleem.

Agressieve failover

Deze optie is standaard ingeschakeld in AireOS WLC's. Als agressieve failover is ingeschakeld, merkt de WLC de AAA-server als niet-responsief en wordt de server verplaatst naar de volgende geconfigureerde AAA-server nadat een RADIUS-time-out-gebeurtenis invloed heeft op één client.

Wanneer de functie is uitgeschakeld, kan de WLC alleen naar de volgende server overschakelen als de RADIUS-tijdelijke gebeurtenis met ten minste 3 clientsessies plaatsvindt. Deze optie kan door deze opdracht worden uitgeschakeld (voor deze opdracht is geen reboot vereist):

```
(Cisco Controller) >config radius aggressive-failover disable
```

U kunt de huidige status van de functie als volgt verifiëren:

```
(Cisco Controller) >show radius summary
```

```
Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

Omleiding voor intern gebruik

De endpoints die een Captive Network Assistant (CNA)-mechanisme ondersteunen om een captive-portal te ontdekken en een aanmeldpagina automatisch te starten doen dit meestal via een pseudo-browser in een gecontroleerd venster terwijl andere endpoints een volledig capabele browser starten om dit te activeren. Voor eindpunten waar CNA een pseudo-browser lanceert, kan dit de stroom breken wanneer omgeleid naar een ISE captive portal. Dit is doorgaans van invloed op Apple IOS-apparaten en het heeft vooral negatieve effecten in stromen die apparaatregistratie, VLAN DHCP-Release, nalevingscontrole vereisen.

De complexiteit van de stroom in gebruik kan worden aanbevolen om Captive Bypass in te schakelen. In een dergelijk scenario negeert de WLC het CNA portaal detectiemechanisme en moet de client een browser openen om het redirect proces te starten.

Controleer de status van de functie:

```
(Cisco Controller) >show network summary

Web Auth CMCC Support ..... Disabled
Web Auth Redirect Ports ..... 80,3128
Web Auth Proxy Redirect ..... Disable
Web Auth Captive-Bypass ..... Disabled
Web Auth Secure Web ..... Enable
Web Auth Secure Redirection ..... Enable
```

U kunt deze opdracht als volgt inschakelen:

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.
```

You must reset system for this setting to take effect.

De WLC waarschuwt de gebruiker dat er een reset-systeem (opnieuw opstarten) nodig is om wijzigingen door te voeren.

Op dit punt toont een **samenvatting van het shownetwerk** de functie zoals ingeschakeld, maar om de wijzigingen van kracht te laten worden moet de WLC opnieuw opgestart worden.

Configureer geconvergeerde 3850 NGWC

Wereldwijde configuratie

1. Wereldwijd ISE toevoegen als een verificatie- en accounting server

- Navigeer naar **Configuratie > Beveiliging > RADIUS > servers** en klik op **Nieuw**
- Voer het **IP-adres** van de ISE-server, het **gedeelde geheim**, de **time-out van de server** en het aantal **nieuwe pogingen** in dat de omgevingsomstandigheden weergeeft.
- Zorg ervoor dat **ondersteuning voor RFC 3570** (CoA-ondersteuning) is ingeschakeld.
- Herhaal het proces om een secundaire serveringang toe te voegen.

RADIUS Servers

Radius Servers > **New**

Server Name

Server IP Address

Shared Secret

Confirm Shared Secret

Auth Port (0-65535)

Acct Port (0-65535)

Server Timeout (1-1000)secs

Retry Count (0-100)

Support for RFC 3576 ▾

2. Servergroep van ISE maken

- Navigeer naar **Configuratie > Beveiliging > Servergroepen** en klik op **Nieuw**
- Wijs een naam toe aan de groep en voer in minuten een **Dode-tijd** waarde in. Dit is de tijd dat de controller de server in de Inactieve wachtrij houdt voordat deze opnieuw wordt gepromoot naar de actieve serverlijst.
- Voeg ze in de lijst Beschikbare servers toe aan de kolom Toegewezen servers.

Radius Server Group

Radius Server Group > **New**

Name

MAC-delimiter ▾

MAC-filtering ▾

Dead-time (0-1440) in minutes

Group Type

Servers In This Group

Available Servers

< >

Assigned Servers

ISE2

ISE1

3. Wereldwijd Dot1x inschakelen

- Navigeer naar **Configuratie > AAA > Methodelijsten > Algemeen** en schakel **Dot1x-systeem** in

General

Dot1x System Auth Control

Local Authentication

Local Authorization

4. Methodelijsten configureren

- Navigeer naar **Configuratie > AAA > Methodelijsten > Verificatie** en maak een nieuwe methodelijst. In dit geval gaat het om Type Dot1x en Group ISE_Group (groep die in de vorige stap is gemaakt). Klik vervolgens op **Toepassen**

Authentication
Authentication > New

Method List Name

Type: dot1x login

Group Type: group local

Fallback to local

Groups In This Method

Available Server Groups

Assigned Server Groups

ISE_Group

- Doe dit ook voor accounting (**Configuratie > AAA > methodelijsten > accounting**) en autorisatie (**Configuratie > AAA > methodelijsten > autorisatie**). Ze moeten er zo uitzien

Accounting
Accounting > New

Method List Name

Type: dot1x exec identity network commands

Groups In This Method

Available Server Groups

Assigned Server Groups

ISE_Group

Authorization
Authorization > New

Method List Name:

Type: network exec credential-download

Group Type: group local

Available Server Groups:

Assigned Server Groups:

Groups In This Method:

5. Maak de MAC-filtermethode voor autorisatie.

Dit wordt later aangeroepen vanuit de SSID-instellingen.

- Navigeer naar **Configuration > AAA > Methodenlijsten > Autorisatie** en klik op **Nieuw**.
- Voer de **naam** van de **methodelijst** in. Kies **type = netwerk-** en **groepstype groep**.
- Voeg **ISE_Group** toe aan het veld **Toegewezen servergroepen**.

Authorization
Authorization > New

Method List Name:

Type: network exec credential-download

Group Type: group local

Available Server Groups:

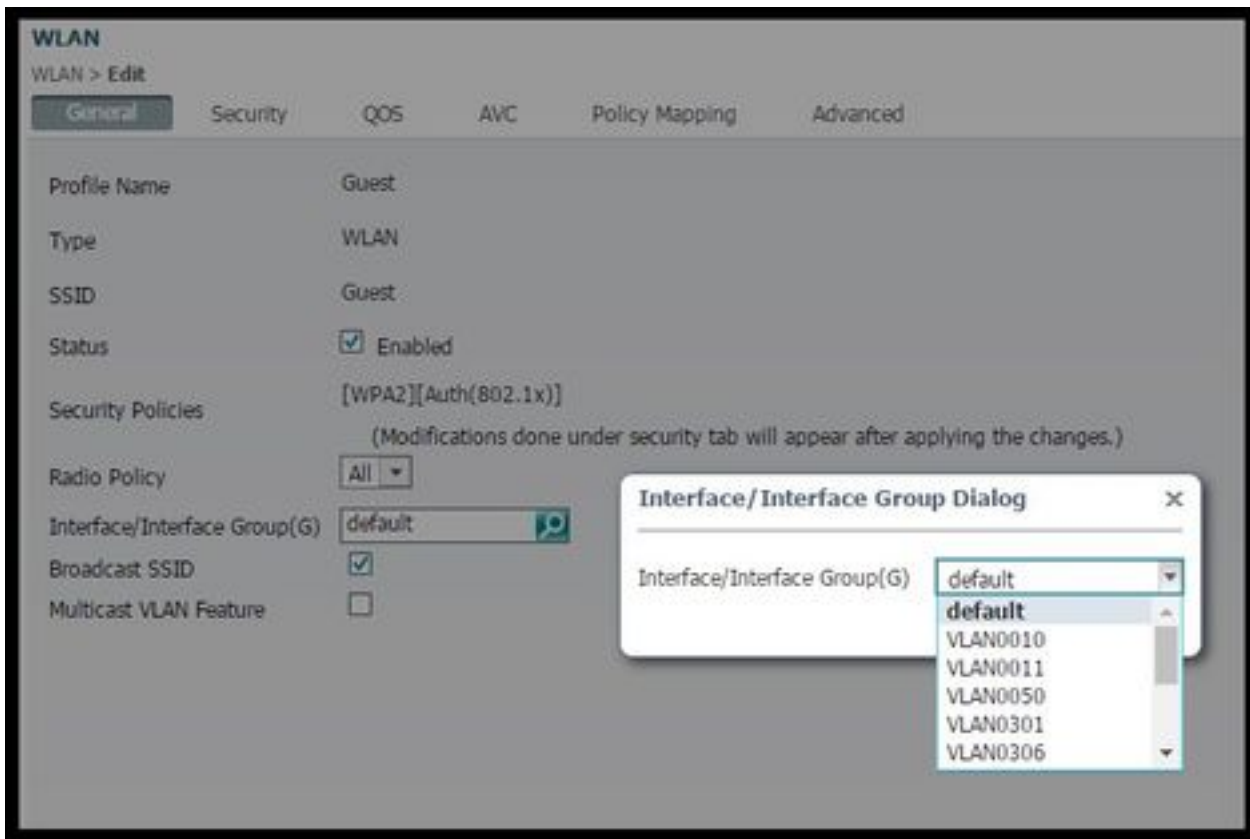
Assigned Server Groups:

Groups In This Method:

SSID-configuratie

1. Maak de gast SSID

- Navigeer naar **Configuratie > Draadloos > WLAN's** en klik op **Nieuw**
- Voer de **WLAN-id**, de **SSID** en de **profielnaam** in en klik op **Toepassen**.
- Selecteer in de **SSID-instellingen** onder **Interface / Interface Group** de interface **Guest VLAN Layer 3**.



- Selecteer onder **Security > Layer 2 Geen** en voer naast **Mac-filtering** de naam van de methodelijst voor Mac-filter in die u eerder hebt geconfigureerd (MacFilterMethod).
- Selecteer onder **Security > AAA Server** Tab de juiste methoden voor verificatie en accounting lijsten (ISE_Method).



- **Schakel** onder het tabblad **Advanced** de status **AAA negeren** en **NAC toe**. De rest van de instellingen moet worden aangepast volgens elke implementatievereisten (sessietime-out, uitsluiting van client, ondersteuning voor Aironet-uitbreidingen).

WLAN
WLAN > Edit

General Security QOS AVC Policy Mapping **Advanced**

Allow AAA Override
 Coverage Hole Detection
 Session Timeout (secs)
 Aironet IE
 Diagnostic Channel
 P2P Blocking Action
 Media Stream Multicast-direct
 Client Exclusion
 Timeout Value(secs)
 Max Allowed Client

DHCP

DHCP Server IP Address
 DHCP Address Assignment required
 DHCP Option 82
 DHCP Option 82 Format
 DHCP Option 82 Ascii Mode
 DHCP Option 82 Rid Mode

NAC

NAC State

- Navigeer naar het tabblad Algemeen en stel de status in op Ingeschakeld. Druk vervolgens op Toepassen.

Configuratie ACL-omleiding

Deze ACL wordt van verwijzingen voorzien door ISE later in toegang-keurt in antwoord op het aanvankelijke verzoek van MAB goed. De NGWC gebruikt het om te bepalen welk verkeer moet worden omgeleid en welk verkeer moet worden toegestaan.

- Navigeer naar configuratie > beveiliging > ACL > toegangscontrolelijsten en klik op Nieuw toevoegen.
- Selecteer Extended en voer de ACL-naam in.
- Dit beeld toont een voorbeeld van typische omleiding ACL:

Access Control Lists
ACLs > ACL detail

Details :

Name: **Guest_Redirect**
 Type: **IPv4 Extended**

Add Sequence Remove

	Seq	Action	Protocol	Source IP/Mask	Destination IP/Mask	Source Port	Destination Port
<input type="radio"/>	10	deny	icmp	any	any	-	-
<input type="radio"/>	20	deny	udp	any	any	-	eq 67
<input type="radio"/>	30	deny	udp	any	any	-	eq 68
<input type="radio"/>	40	deny	udp	any	any	-	eq 53
<input type="radio"/>	50	deny	tcp	any	████████.157.210	-	eq 8443
<input type="radio"/>	60	deny	tcp	any	████████.157.21	-	eq 8443
<input type="radio"/>	70	permit	tcp	any	any	-	eq 80
<input type="radio"/>	80	permit	tcp	any	any	-	eq 443

Opmerking: lijn 10 is niet verplicht. Dit wordt meestal toegevoegd voor het oplossen van problemen. Deze ACL moet toegang verlenen tot DHCP-, DNS-services en ook tot ISE-serverpoort TCP 8443 (Deny ACE's). HTTP- en HTTPS-verkeer wordt omgeleid (toestemming voor ACE's).

CLI-configuratie (Command-Line Interface)

Alle configuratie die in de vorige stappen is besproken, kan ook via de CLI worden toegepast.

802.1x wereldwijd ingeschakeld

```
dot1x system-auth-control
```

Wereldwijde AAA-configuratie

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa authorization network MacFilterMethod group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
  client 172.16.157.210 server-key *****
  client 172.16.157.21 server-key *****
  auth-type any
!
radius server ISE1
  address ipv4 172.16.157.210 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
radius server ISE2
  address ipv4 172.16.157.21 auth-port 1812 acct-port 1813
  timeout 5
  retransmit 2
  key *****
!
!
aaa group server radius ISE_Group
  server name ISE2
  server name ISE1
  deadtime 10
  mac-delimiter colon
!
```

WLAN-configuratie

```
wlan Guest 1 Guest
aaa-override
accounting-list ISE_Method
client vlan VLAN0301
mac-filtering MacFilterMethod
nac
```



```
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security dot1x authentication-list ISE_Method
no security ft over-the-ds
session-timeout 28800
no shutdown
```

Voorbeeld ACL-omleiding

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
 10 deny icmp any any
 20 deny udp any any eq bootps
 30 deny udp any any eq bootpc
 40 deny udp any any eq domain
 50 deny tcp any host 172.16.157.210 eq 8443
 60 deny tcp any host 172.16.157.21 eq 8443
 70 permit tcp any any eq www
 80 permit tcp any any eq 443
```

HTTP- en HTTPS-ondersteuning

```
3850#show run | inc http
ip http server
ip http secure-server
```

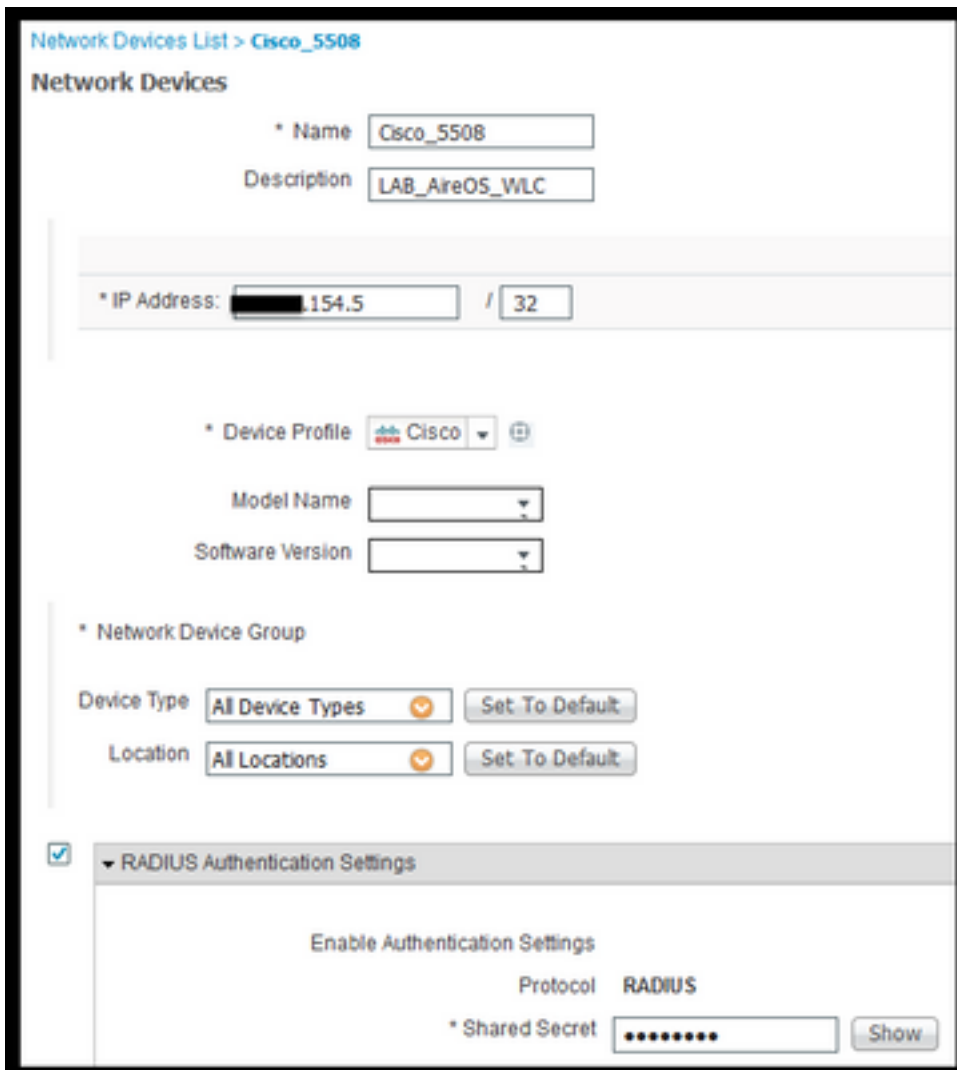
Opmerking: als u een ACL toepast om de toegang tot de WLC via HTTP te beperken, heeft dit gevolgen voor de omleiding.

ISE configureren

In deze sectie wordt de configuratie beschreven die op ISE is vereist om de alle gebruikscases te ondersteunen die in dit document worden besproken.

Gemeenschappelijke ISE-configuratie-taken

1. Log in op ISE en navigeer naar **Beheer > Netwerkbronnen > Netwerkkapparaten** en klik op **Toevoegen**
2. Voer de **naam in** die aan de WLC en het **IP-adres** van het apparaat is gekoppeld.
3. Controleer het vakje **RADIUS-verificatie-instellingen** en typ het **gedeelde geheim dat** aan de WLC-zijde is geconfigureerd. Klik vervolgens op **Indienen**.

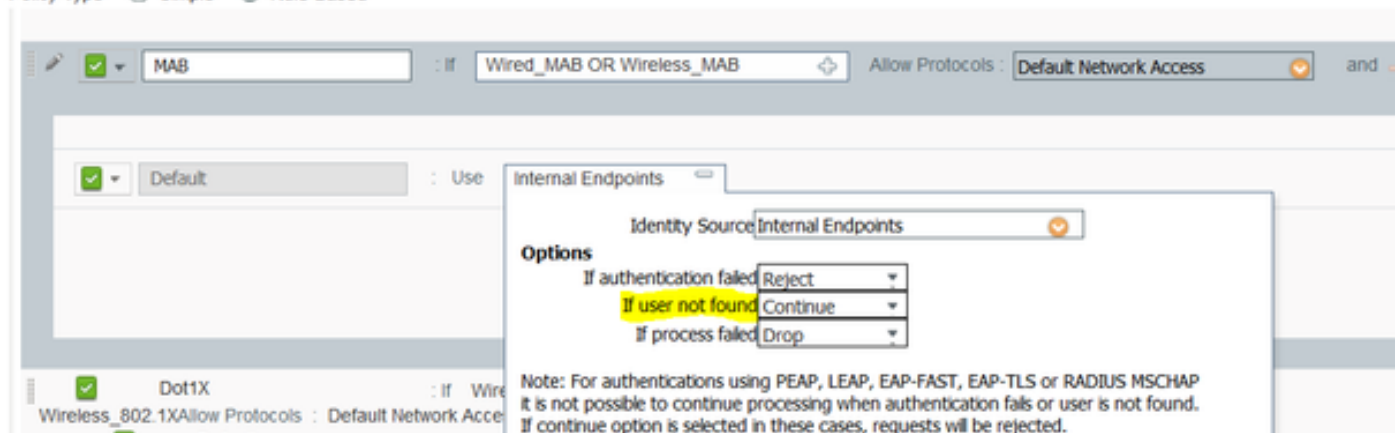


4. Navigeer naar **Beleid > Verificatie** en klik onder **MAB** op **Bewerken** en zorg ervoor dat onder **Gebruik: Interne endpoints** de optie **Als gebruiker niet gevonden is**, wordt ingesteld op **Doorgaan** (deze moet standaard aanwezig zijn).

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication. For Policy Export go to [Administration > System > Backup & Restore > Policy Export Page](#)

Policy Type Simple Rule-Based



Use case 1: CWA met gastverificatie in elke gebruikersverbinding

Flow - Overzicht

1. Draadloze gebruiker maakt verbinding met de Guest SSID.

2. WLC verifieert het eindpunt op basis van zijn MAC-adres op ISE als AAA-server.
3. ISE retourneert terug en accepteert toegang met twee Attribute Value Pairs (AVP's): url-redirect en url-redirect-acl. Zodra de WLC deze AVP's toepast op de endpointssessie, gaat het station over naar DHCP-Vereist en zodra het een IP-adres invoegt, blijft het in CENTRAL_WEB_AUTH. Bij deze stap is de WLC klaar om het http / https-verkeer van de client om te leiden.
4. De eindgebruiker opent de webbrowser en zodra HTTP- of HTTPS-verkeer is gegenereerd, stuurt de WLC de gebruiker naar ISE guest portal.
5. Zodra de gebruiker bij de Guest Portal komt, wordt gevraagd om de gastreferenties (in dit geval door de sponsor gemaakt) in te voeren.
6. Op geloofsbrieven toont de bevestiging ISE de AUP pagina en zodra de client accepteert, wordt een Dynamic CoA type opnieuw-authenticeren verzonden naar de WLC.
7. De WLC verwerkt de MAC-filtering-verificatie opnieuw zonder een deauthenticate uit te geven aan het mobiele station. Dit moet naadloos zijn tot het eindpunt.
8. Zodra de herauthenticatie gebeurtenis gebeurt, herevalueert ISE het autorisatiebeleid en dit keer wordt het eindpunt een Permit-toegang gegeven omdat er een eerdere succesvolle gast-authenticatie-gebeurtenis was.

Dit proces herhaalt zich elke keer dat de gebruiker verbinding maakt met de SSID.

Configuratie

1. Navigeer naar ISE en navigeer naar **Work Centers > Guest Access > Configure > Guest Portals > Select Sponsored Guest Portal** (of maak een nieuw portaal type Sponsored-Guest).
2. Schakel alle opties uit onder **Instellingen voor registratie van gastapparaat** en klik op **Opslaan**.



3. Navigeer naar **Beleid > Beleidselementen > Resultaten > Vergunning > Vergunningsprofielen**. Klik op **Add** (Toevoegen).

4. Dit profiel wordt naar beneden geduwd naar de WLC de **Redirect-URL** en de **Redirect-URL-ACL** in antwoord op het eerste Mac-authenticatie bypass (MAB) verzoek.

- Zodra de omleiding van het Web (CWA, MDM, NSP, CPP) selecteerde uitgezocht Gecentraliseerde Web Auth, dan Type de Redirect ACL naam onder ACL-veld en onder **Waarde** selecteer de **Gesponsorde Gast Portal (gebrek)** (of een ander specifiek portaal dat in vorige stappen is gemaakt).

Het profiel moet er hetzelfde uitzien als in deze afbeelding. Klik vervolgens op **Opslaan**.

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

Common Tasks

Web Redirection (CWA, MDM, NSP, CPP) (i)

Centralized Web Auth ACL Value

Display Certificates Renewal Message

Static IP/Host name/FQDN

Attribute Details onderaan de pagina Attribute Value Pairs (AVP's), aangezien deze naar de WLC worden gedrukt

Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = url-redirect-acl=Guest_Redirect
cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a65b8890-2230-11e6-99ab-005056bf55e0&daysToExpiry=value&action=cwa
```

5. Navigeer naar **Beleid > Autorisatie** en voer een nieuwe regel in. Deze regel is degene die het redirect proces in reactie op het eerste MAC-authenticatieverzoek van WLC activeert. (In dit geval **Wireless_Guest_Redirect** genoemd).

6. Onder **Voorwaarden** kies **Selecteer Bestaande Voorwaarden uit Bibliotheek**, dan onder **Conditionenaam** selecteer **Samengestelde voorwaarde**. Selecteer een vooraf gedefinieerde samengestelde voorwaarde genaamd **Wireless_MAB**.

Opmerking: deze voorwaarde bestaat uit 2 Radius-kenmerken die worden verwacht in het toegangsverzoek dat is voortgekomen uit de WLC (NAS-Port-Type= IEEE 802.11 <aanwezig in alle draadloze aanvragen> en Service-Type = Call Check< die verwijst naar een specifiek verzoek om een mac-verificatie-bypass>)

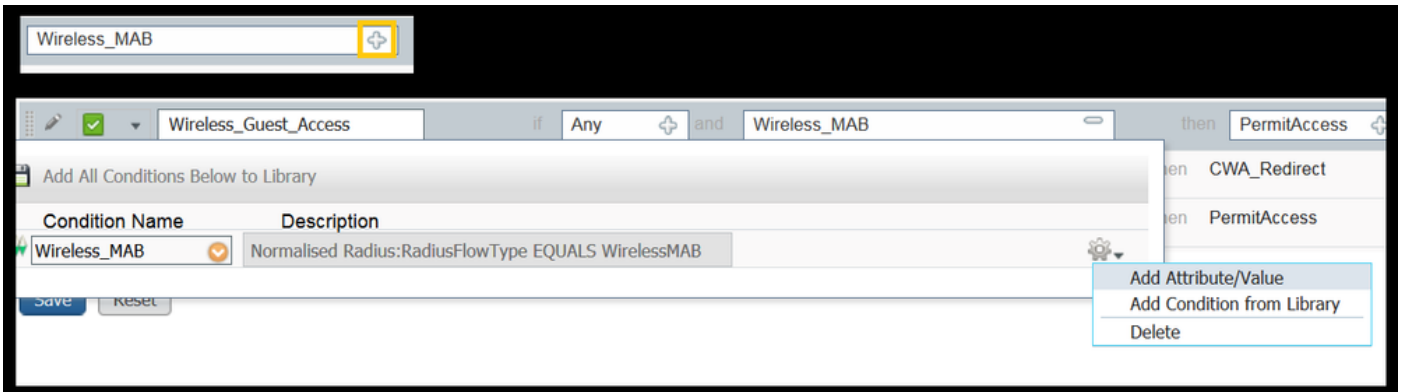
7. Selecteer onder resultaten **Standard > CWA_Redirect** (Autorisatieprofiel gemaakt in vorige stap). Klik vervolgens op **Gereed** en opslaan

Wireless_Guest_Redirect if Wireless_MAB then CWA_Redirect [Edit](#)

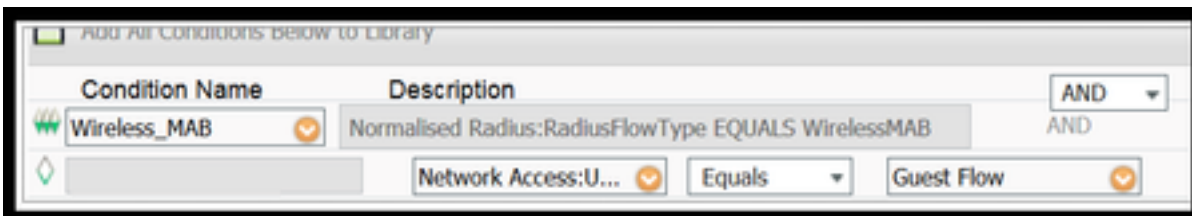
8. Navigeer naar het einde van de **CWA_Redirect** regel en klik op het pijltje naast **Bewerken**. Selecteer vervolgens **hierboven het duplicaat**.

9. Wijzig de naam aangezien dit het beleid is dat het eindpunt aanpast zodra de sessie opnieuw is geverifieerd op de CoA van ISE (in dit geval Wireless_Guest_Access).

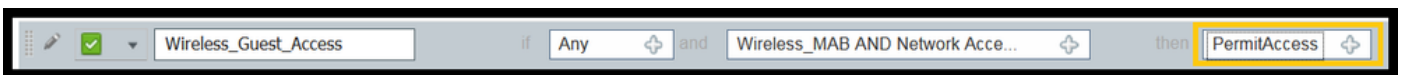
10. Klik naast **Wireless_MAB** verbinding voorwaarde op het + symbool om de voorwaarden uit te vouwen en klik tegen het eind van de **Wireless_MAB** voorwaarde op **Add Attribute/Value**.



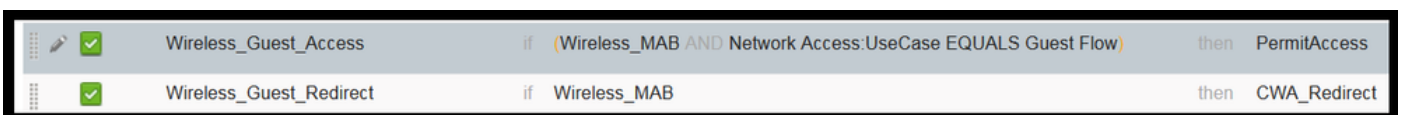
11. Selecteer onder "Kenmerk selecteren" de optie **Netwerktoegang > UseCase = Gaststroom**



12. Selecteer onder **Toestemmingen** de optie **Toegang verlenen**. Klik vervolgens op **Gereed** en **opslaan**



De twee beleidsterreinen moeten er als volgt uitzien:



Use case 2: CWA met apparaatregistratie die de gastenverificatie eenmaal per dag uitvoert.

Flow - Overzicht

1. Draadloze gebruiker maakt verbinding met de Guest SSID.
2. WLC verifieert het eindpunt op basis van zijn MAC-adres op ISE als AAA-server.
3. ISE retourneert en accepteert met twee Attribute Value Pairs (AVP's) (url-redirect en url-redirect-acl).
4. Zodra de WLC deze AVP's toepast op de endpointsessie, gaat het station over naar DHCP-Vereist en zodra het een IP-adres invoegt, blijft het in CENTRAL_WEB_AUTH. Bij deze stap is de WLC klaar om het http / https-verkeer van de client om te leiden.
5. De eindgebruiker opent de webbrowser en zodra HTTP- of HTTPS-verkeer is gegenereerd, stuurt de WLC de gebruiker naar ISE guest portal.
6. Zodra de gebruiker bij de Guest Portal komt, wordt hij gevraagd om door sponsor gemaakte

referenties in te voeren.

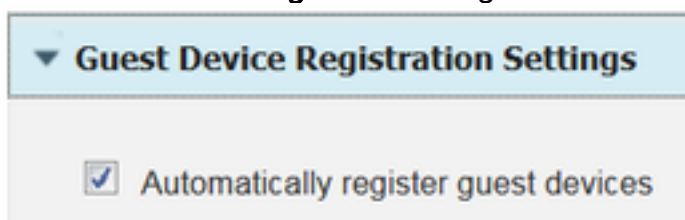
7. Bij het valideren van referenties voegt ISE dit eindpunt toe aan een specifieke (vooraf geconfigureerde) Endpoint Identity Group (Apparaatregistratie).
8. De AUP-pagina wordt weergegeven en zodra de client deze accepteert, wordt een Dynamic CoA-type opnieuw geverifieerd. Wordt verzonden naar de WLC.
9. De WLC om de MAC filtering verificatie opnieuw te verwerken zonder een deauthenticate uit te geven aan het mobiele station. Dit moet naadloos zijn tot het eindpunt.
10. Zodra de re authenticatie gebeurtenis gebeurt, herevalueert ISE autorisatiebeleid. Dit keer omdat het eindpunt lid is van de juiste Endpoint Identity Group ISE retourneert een toegang accepteren zonder beperkingen.
11. Aangezien het eindpunt in stap 6 is geregistreerd, wordt elke keer dat de gebruiker terugkomt, hij toegestaan op het netwerk tot het handmatig uit ISE wordt verwijderd, of een Endpoint Purge Policy voert het doorspoelen van de endpoints die aan de criteria voldoen uit.

In dit laboratoriumscenario wordt de authenticatie eenmaal per dag afgedwongen. Reauthenticatie trigger is Endpoint Purge Policy die alle endpoints van de gebruikte Endpoint Identity Group elke dag verwijdert.

Opmerking: het is mogelijk om de gast authenticatie-event af te dwingen op basis van Verlopen tijd sinds de laatste AUP-acceptatie. Dit kan een optie zijn als u de Gastenaanmelding vaker dan eenmaal per dag (bijvoorbeeld elke 4 uur) moet afdwingen.

Configuratie

1. Op ISE navigeer naar **Work Centers > Guest Access > Configure > Guest Portals > Select Sponsored Guest Portal** (of maak een nieuw portaal type Sponsored-Guest).
2. Controleer onder **Instellingen voor registratie van gastapparaten** of de optie **Gastapparaten automatisch registreren** is ingeschakeld. Klik op **Save** (Opslaan).



3. Navigeer naar het **werkcentrum > Gasttoegang > Configureren > Gasttypes** of klik op de sneltoets die is opgegeven onder Instellingen voor registratie van gastapparaten in het portaal.

▼ Guest Device Registration Settings

Automatically register guest devices

A message displays to guests when they reach the maximum number of supported devices.

Allow guests to register devices

You can set the maximum number of supported devices in the guest type settings.

Device information will be stored in the endpoint identity group specified in the guest type of the user logging in to this portal.

Configure guest types at:

[Work Centers > Guest Access > Configure > Guest Types](#)

4. Wanneer de Sponsor-gebruiker een gastaccount aanmaakt, wijst hij er een gasttype aan toe. Elk individueel gasttype kan een geregistreerd eindpunt hebben dat tot een andere Endpoint Identity Group behoort. Om de Endpoint Identity Group toe te wijzen moet het apparaat worden toegevoegd, selecteert u het gasttype dat de sponsor voor deze gastgebruikers gebruikt (Deze gebruikscase is gebaseerd op Weekly (standaard)).

5. Eenmaal in het gasttype selecteert u onder **Aanmeldingsopties** de Endpoint Group in het keuzemenu **Endpoint Identity group voor registratie van het gastapparaat**

Maximum devices guests can register: (1-999)

Endpoint identity group for guest device registration: ⓘ

6. Navigeer naar **Beleid > Beleidselementen > Resultaten > Vergunning > Vergunningsprofielen**. Klik op **Add** (Toevoegen).

7. Dit profiel wordt naar beneden geduwd naar de WLC de **Redirect-URL** en de **Redirect-URL-ACL** in antwoord op het eerste Mac-authenticatie bypass (MAB) verzoek.

- Zodra de omleiding van het Web (CWA, MDM, NSP, CPP) controleerde uitgezocht **Gecentraliseerde Web Auth**, dan Type de Redirect ACL naam onder **ACL-veld** en onder **Waarde** selecteer het portaal dat voor deze stroom wordt gemaakt (**CWA_DeviceRegistration**).

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

▼ Common Tasks

VLAN

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Centralized Web Auth ACL Value

8. Navigeer naar **Beleid > Autorisatie** en voer een nieuwe regel in. Deze regel is degene die het redirect proces in reactie op het eerste MAC-authenticatieverzoek van WLC activeert. (In dit geval **Wireless_Guest_Redirect** genoemd).

9. Onder **Voorwaarden** kies **Selecteer Bestaande Voorwaarden uit bibliotheek**, dan onder **Conditionenaam** selecteer **Samengestelde voorwaarde**. Selecteer een vooraf gedefinieerde samengestelde voorwaarde genaamd **Wireless_MAB**.

10. Selecteer onder resultaten de optie **Standaard > CWA_DeviceRegistration** (Autorisatieprofiel gemaakt in vorige stap). Klik vervolgens op **Gereed** en **opslaan**

Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

11. Dubbel het bovenstaande beleid, wijzig de naam ervan omdat dit het beleid is dat het eindpunt raakt nadat het is teruggekeerd van de herverificatiegebeurtenis (genaamd **Wireless_Guest_Access**).

12. Selecteer onder het vakje **Identity Group Details** de optie **Endpoint Identity Group** en selecteer de groep waarnaar u verwijst onder het gasttype (GuestEndpoints).

13. Selecteer onder Resultaten de optie **Toegang toestaan**. Klik op **Gereed** en **sla** de wijzigingen op.

Wireless_Guest_Access if GuestEndpoints AND Wireless_MAB then PermitAccess
 Wireless_Guest_Redirect if Wireless_MAB then CWA_DeviceRegistration

14. Maak een eindpunt zuiveringsbeleid dat de GuestEndpoint Group dagelijks ontruimt.

- Navigeren naar **Beheer > Identity Management > Instellingen > Opschonen van endpoints**
- Onder de regels van de **Zuivering** moet er één door gebrek zijn dat de verwijdering van GuestEndpoints teweegbrengt als Verlopen Tijd meer dan 30 dagen is.
- Wijzig het bestaande beleid voor GuestEndpoints of maak een nieuwe beleid (voor het geval dat de standaard is verwijderd). Merk op dat het zuiveringsbeleid elke dag binnen een bepaalde tijd wordt uitgevoerd.


In dit geval is de voorwaarde leden van GuestEndpoints met Verlopen Dagen minder dan 1 dag

Use case 3: hostspotportal

Flow - Overzicht

1. Draadloze gebruiker maakt verbinding met de Guest SSID.
2. WLC verifieert het eindpunt op basis van zijn MAC-adres met ISE als AAA-server.
3. ISE retourneert een access-acceptatie met twee Attribute Value Pairs (AVP's): url-redirect en url-redirect-acl.
4. Zodra de WLC deze AVP's toepast op de endpointsessie, gaat het station over naar DHCP-Vereist en zodra het een IP-adres invoegt, blijft het in CENTRAL_WEB_AUTH. Bij deze stap is WLC bereid om het http / https-verkeer van de klant om te leiden.
5. De eindgebruiker opent de webbrowser en zodra HTTP- of HTTPS-verkeer is gegenereerd, leidt de WLC de gebruiker naar ISE HotSpot Portal.
6. Eenmaal in de portal wordt de gebruiker gevraagd om een beleid voor acceptabel gebruik te accepteren.
7. ISE voegt het MAC-adres (Endpoint-id) toe aan de geconfigureerde Endpoint Identity-groep.
8. Het Policy Services Node (PSN) dat het verzoek verwerkt, geeft een Dynamic CoA-type **Admin-Reset** aan de WLC uit.
9. Zodra de WLC klaar is met het verwerken van de inkomende CoA, geeft het een ont-authenticeren aan de client uit (verbinding is verlies voor tijd het duurt voor de client terug te komen).
10. Zodra de client opnieuw verbinding maakt, wordt een nieuwe sessie aangemaakt, zodat er geen sessiecontinuïteit is aan de kant van ISE. Het betekent dat de authenticatie verwerkt wordt als een nieuwe thread.
11. Aangezien het eindpunt wordt toegevoegd aan de geconfigureerde Endpoint Identity Group en er een autorisatiebeleid is dat controleert of het eindpunt deel uitmaakt van die groep, komt de nieuwe verificatie overeen met dit beleid. Het resultaat is volledige toegang tot het gastennetwerk.
12. De gebruiker hoeft de AUP niet opnieuw te accepteren, tenzij het Endpoint Identity Object uit de ISE-database wordt gewist als gevolg van een beleid voor het wissen van eindpunten.

Configuratie

1. Maak een nieuwe endpointgroep om deze apparaten bij registratie naar te verplaatsen. Navigeren naar **werkcentra > Gasttoegang > Identiteitsgroepen > Endpoint Identity Groups** en klik op  .
- Voer een groepsnaam in (in dit geval HotSpot_Endpoints). Voeg een beschrijving toe en er is geen Parent Group nodig.

Endpoint Identity Group List > HotSpot_Endpoints

Endpoint Identity Group

* Name

Description

Parent Group

2. Navigeren naar **werkcentra > Gasttoegang > Configureren > Gastportalen > Hotspot-portal** selecteren (**standaard**).

3. Poortinstellingen uitvouwen en onder Endpoint Identity Group selecteert u **HotSpot_Endpoints** groep onder **Endpoint Identity Group**. De geregistreerde apparaten worden nu naar de opgegeven groep verzonden.

Endpoint

Identity *Configure endpoint identity groups at:*

group: * [Work Centers > Guest Access > Identity Groups](#)

4. Sla de wijzigingen op.

5. Maak het autorisatieprofiel dat het HotSpot Portal aanroept op MAB-verificatie die is voortgekomen uit de WLC.

- Navigeer naar **Beleid > Beleidselementen > Resultaten > autorisatie > Autorisatieprofielen** en maak er een (HotSpotRedirect).
- Zodra de **omleiding van het Web (CWA, MDM, NSP, CPP)** wordt gecontroleerd selecteer **Hot Spot**, dan typ de Redirect ACL naam in ACL-veld (Guest_Redirect) en als Waarde selecteer juiste portal (**Hotspot Portal (standaard)**).

Add New Standard Profile

Authorization Profile

* Name:

Description:

* Access Type:

Network Device Profile:

Common Tasks

Voice Domain Permission

Web Redirection (CWA, MDM, NSP, CPP) ⓘ

Hot Spot: ACL: Value:

Static IP/Host name/FQDN

Attributes Details

Access Type = ACCESS_ACCEPT
 cisco-av-pair = url-redirect-ad=Guest_Redirect
 cisco-av-pair = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=a60e04d0-2230-11e6-99ab-005056bf55e0&action=cwa&type=drw

6. Maak het autorisatiebeleid dat het HotSpotRedirect resultaat activeert op eerste MAB aanvraag van WLC.

- Navigeer naar **Beleid > Autorisatie** en voeg een nieuwe regel in. Deze regel is degene die het omleiden proces in reactie op het eerste MAC-verificatieverzoek van WLC activeert. (In dit geval **Wireless_HotSpot_Redirect** genoemd).
- Kies onder **Voorwaarden Bestaande Voorwaarden uit bibliotheek selecteren**, en selecteer onder **conditienaam Samengestelde voorwaarde**
- Selecteer onder resultaten de optie **Standaard > HotSpotRedirect** (Autorisatieprofiel gemaakt in vorige stap). Klik vervolgens op **Gereed** en **opslaan**

7. Maak het tweede autorisatiebeleid aan.

- Dupliceer het bovenstaande beleid, wijzig de naam omdat dit het beleid is dat het eindpunt raakt nadat het is teruggekomen van de herauthenticatie-gebeurtenis (genaamd **Wireless_HotSpot_Access**).
- Selecteer onder het vakje **Identity Group Details** de optie **Endpoint Identity Group** en vervolgens de groep die u eerder hebt gemaakt (**HotSpot_Endpoints**).
- Selecteer onder Resultaten de optie **Toegang toestaan**. Klik op **Gereed** en **sla** de wijzigingen op.

<input checked="" type="checkbox"/>	Wireless_HotSpot_Access	if HotSpot_Endpoints AND Wireless_MAB	then PermitAccess
<input checked="" type="checkbox"/>	Wireless_HotSpot_Redirect	if Wireless_MAB	then HotSpotRedirect

8. Configureer het opschoningsbeleid dat eindpunten met een Verlopen tijd van meer dan 5 dagen ontruimt.

- Ga naar **Beheer > Identity Management > Instellingen > Endpoint Purge** en creëer onder Purge-regels een nieuwe.
- Selecteer onder het vakje **Identity Group Details** de optie **Endpoint Identity Group > HotSpot_Endpoints**

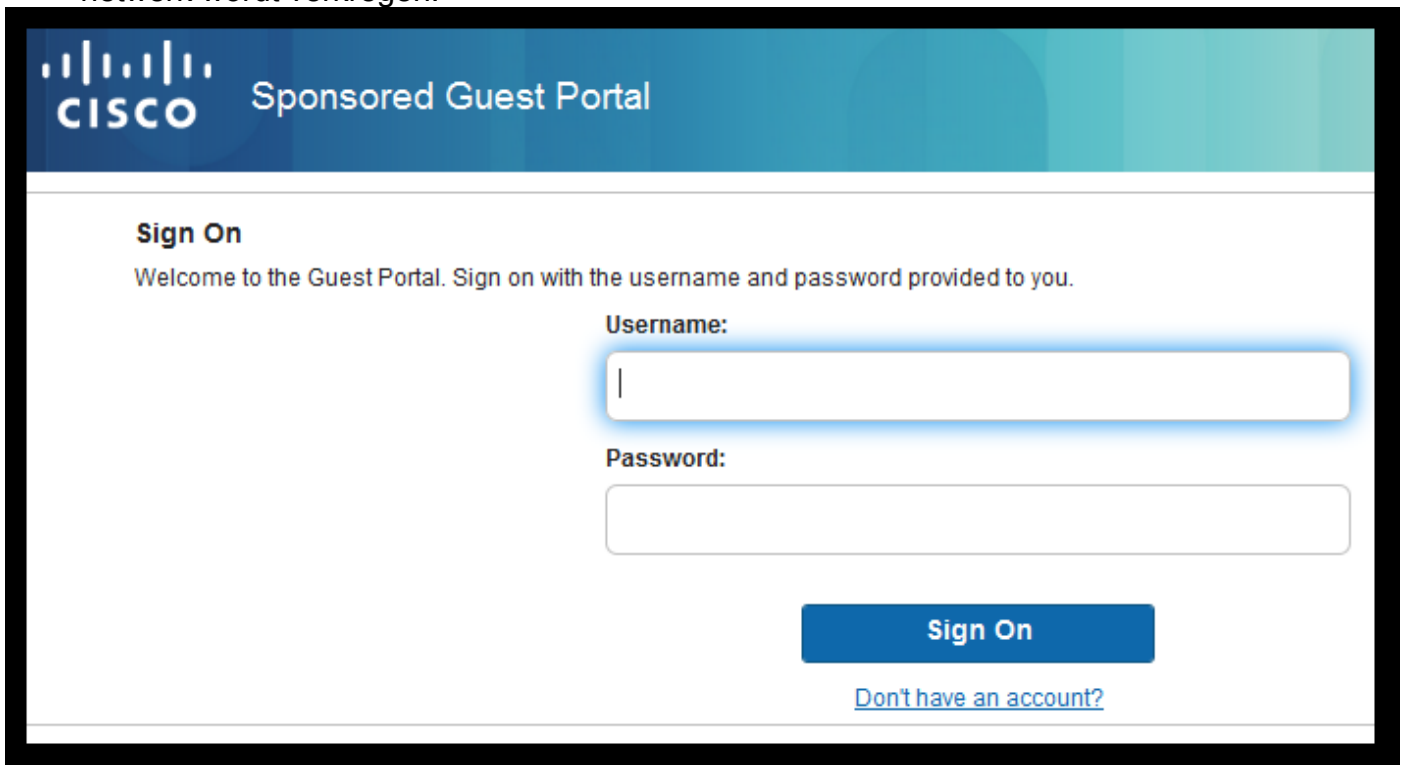
- Klik onder **deze omstandigheden** op **Nieuwe voorwaarde maken (geavanceerde optie)**.
- Kies onder Selecteer Attribuut **ENDPOINTPURGE: ElapsedDays GREATER THAN 5 days**

HotSpot_Endpoints_PurgeRule if **HotSpot_Endpoints** AND ENDPOINTPURGE:ElapsedDays GREATER THAN 5

Verifiëren

Use Case 1

1. Gebruiker maakt verbinding met de Guest SSID.
2. Hij opent de browser en zodra HTTP-verkeer wordt gegenereerd, wordt het gastportaal weergegeven.
3. Zodra de gastgebruiker de AUP heeft geverifieerd en geaccepteerd, wordt er een succespagina weergegeven.
4. Er wordt een Reauthenticate CoA verstuurd (transparant naar de client).
5. De endpointsessie wordt opnieuw geverifieerd als u volledige toegang tot het netwerk hebt.
6. Elke volgende gastverbinding moet de gastverificatie doorstaan voordat toegang tot het netwerk wordt verkregen.



The screenshot shows the Cisco Sponsored Guest Portal sign-on interface. At the top left is the Cisco logo and the text "Sponsored Guest Portal". Below this is a "Sign On" heading followed by the instruction: "Welcome to the Guest Portal. Sign on with the username and password provided to you." There are two input fields: "Username:" and "Password:". Below the password field is a blue "Sign On" button. At the bottom right, there is a link that says "Don't have an account?".



Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline



Success

You now have Internet access through this network.

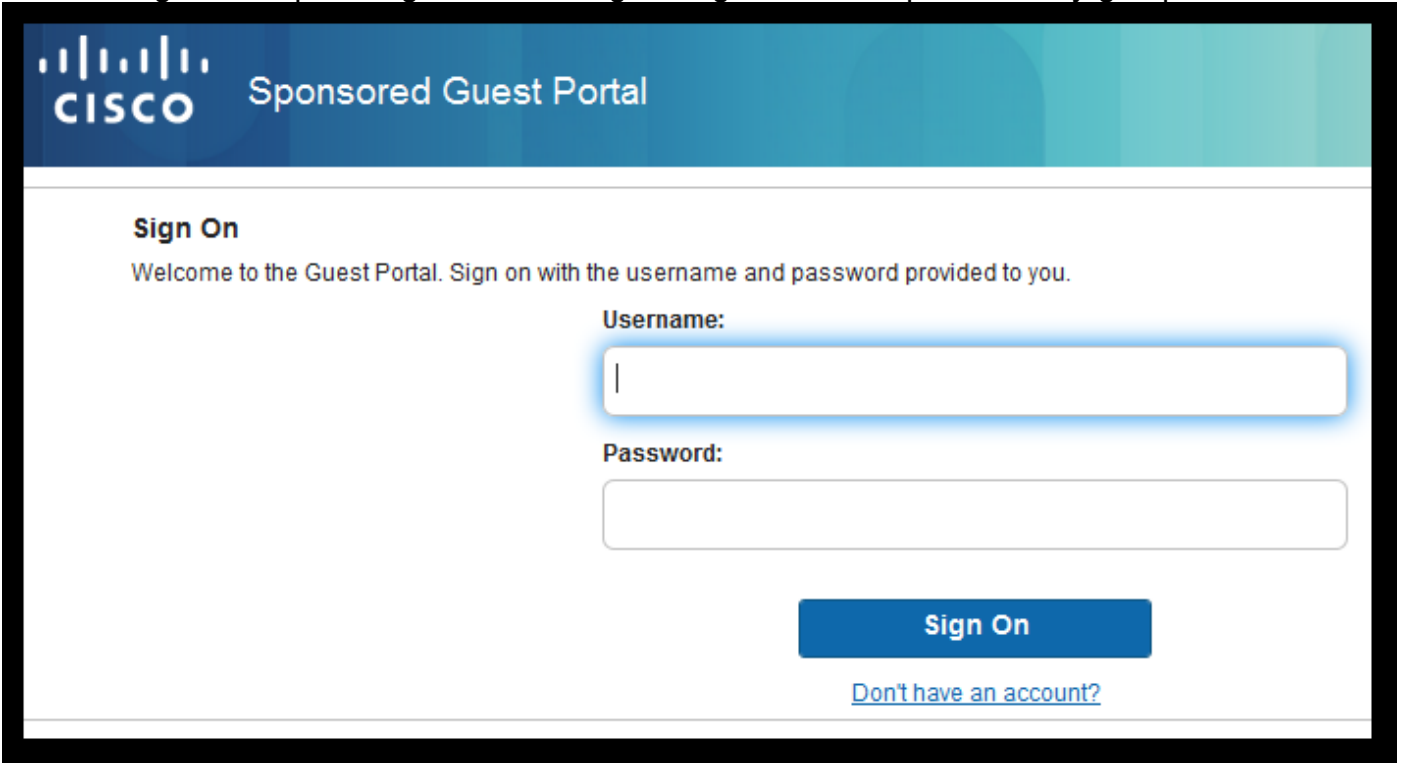
Flow van ISE RADIUS Live logs:

🔍	🔍	1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Accounting Start
✅	🔍	1001	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MAB	Default >> Wir...	PermitAccess	← Re-Authentication Event
✅	🔍		68:7F:74:72:18:2E					← CoA Event
✅	🔍	1001	68:7F:74:72:18:2E					← Guest Authentication Event
✅	🔍	68:7F:74:72:18:2E	68:7F:74:72:18:2E	Windows7-Wo...	Default >> MA...	Default >> Wir...	CWA_Redirect	← Initial MAB request

Use Case 2

1. Gebruiker maakt verbinding met de Guest SSID.
2. Hij opent de browser en zodra HTTP-verkeer wordt gegenereerd, wordt het gastportaal weergegeven.

3. Nadat de gastgebruiker de AUP heeft geverifieerd en geaccepteerd, wordt het apparaat geregistreerd.
4. Er wordt een succespagina weergegeven en er wordt een opnieuw geverifieerde CoA verzonden (transparant naar de client).
5. De endpointsessie wordt opnieuw geverifieerd als u volledige toegang tot het netwerk hebt.
6. Elke volgende gokverbinding 9s toegestaan zonder het afdwingen van gastenverificatie, zolang het eindpunt nog steeds in de geconfigureerde Endpoint Identity-groep zit.



The image shows a screenshot of the Cisco Sponsored Guest Portal. The header features the Cisco logo and the text "Sponsored Guest Portal". Below the header, the page is titled "Sign On" and includes a welcome message: "Welcome to the Guest Portal. Sign on with the username and password provided to you." There are two input fields: "Username:" and "Password:". The "Username:" field is currently empty and has a blue glow effect. Below the "Password:" field is a blue "Sign On" button. At the bottom, there is a link that says "Don't have an account?".

Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

Sign On

[Don't have an account?](#)



Acceptable Use Policy

Please read the Acceptable Use Policy

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or

Accept

Decline

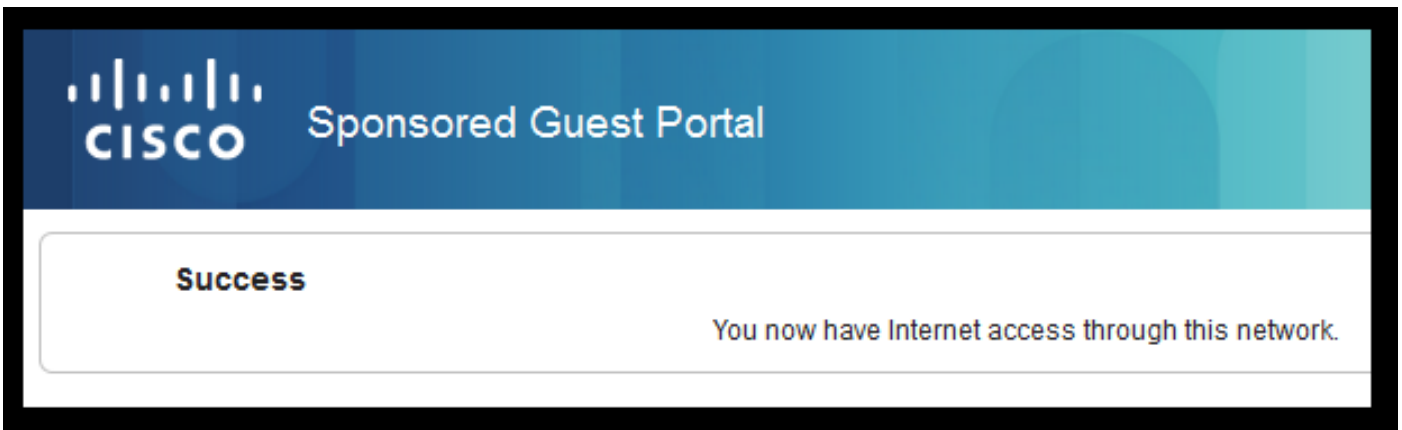


Welcome Message

Click **Continue** to connect to the network.

You're very close to gaining network access.

Continue



Flow van ISE RADIUS Live logs:

Status	Details	Identity	Endpoint ID	Authorization Profiles	Identity Group
		68:7F:74:72:1...	68:7F:74:72:...	PermitAccess	
		68:7F:74:72:1...	68:7F:74:72:...	PermitAccess	GuestEndpoints
		hfr592	68:7F:74:72:...	PermitAccess	User Identity Groups:GuestType_Contractor (default)...
			68:7F:74:72:...		
		hfr592	68:7F:74:72:...		GuestType_Contractor (default)
		68:7F:74:72:1...	68:7F:74:72:...	CWA_DeviceRegistration	Profiled

Accounting Start
 Subsequent MAB request(no redirect to guest portal)
 Re-Authentication Event
 CoA Reauth Event
 Guest Authentication and Device Registration
 Initial MAB request

Use Case 3

1. Gebruiker maakt verbinding met de Guest SSID.
2. Hij opent de browser en zodra HTTP-verkeer wordt gegenereerd, wordt er een AUP-pagina weergegeven.
3. Zodra de gastgebruiker de AUP accepteert, wordt het apparaat geregistreerd.
4. Er wordt een succespagina weergegeven en een Admin-Reset CoA wordt verzonden (transparant naar de client).
5. Het eindpunt wordt opnieuw verbonden met volledige toegang tot het netwerk.
6. Elke volgende gloedverbinding is toegestaan zonder dat de AUP-acceptatie (tenzij anders is ingesteld) wordt afgedwongen zolang het eindpunt in de geconfigureerde Endpoint Identity-groep blijft.



Acceptable Use Policy

Please read the Acceptable Use Policy.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision, amendment, or modification will be posted on Cisco System's website and will be effective as to existing users 30 days after posting.

Accept

Decline



Connection Successful

You have successfully connected to the network.

FlexConnect lokale switching in AireOS

Wanneer FlexConnect lokale switching is geconfigureerd, moet de netwerkbeheerder ervoor zorgen dat:

- Redirect ACL wordt geconfigureerd als FlexConnect ACL.
- Redirect ACL is toegepast als een beleid via het toegangspunt zelf onder het tabblad **FlexConnect > Externe webverificatie ACL's > Beleid > Selecteer Redirect ACL** en klik op **Toepassen**

All APs > Details for aaa-ap-3

General Credentials Interfaces High Availability Inventory **FlexConnect** Advanced

VLAN Support

Native VLAN ID 301 **VLAN Mappings**

FlexConnect Group Name Not Configured

PreAuthentication Access Control Lists

External WebAuthentication ACLs

Local Split ACLs

Central DHCP Processing

Layer2 ACLs

Policies

Policy ACL CWA_Redirect **Add**

Policy Access Control Lists

CWA_Redirect

Of door de Policy ACL toe te voegen aan de FlexConnect-groep waartoe hij behoort (**Wireless > FlexConnect-groepen > Selecteer de juiste groep > ACL-toewijzing > Beleid** Selecteer de Redirect ACL en klik op Toevoegen)

FlexConnect Groups > Edit 'test'

General Local Authentication Image Upgrade **ACL Mapping** Central DHCP WLAN VLAN mapping

AAA VLAN-ACL mapping WLAN-ACL mapping **Policies**

Policies

Policy ACL CWA_Redirect **Add**

Policy Access Control Lists

CWA_Redirect

TOR_Redirect

Door toevoeging van beleidstoegangscontrolelijsten wordt de WLC geactiveerd om de geconfigureerde ACL naar beneden te drukken naar de AP(s)-leden van de FlexConnect-groep. Als u dit niet doet, wordt een probleem via een web omgeleid.

buitenlands ankerscenario

In auto-anker (buitenlands-anker) scenario's is het belangrijk om deze feiten te benadrukken:

- Redirect ACL moet worden gedefinieerd op zowel de Foreign als de Anker WLC. Zelfs als het alleen op het anker wordt afgedwongen.
- Layer 2-verificatie wordt altijd verwerkt door de Foreign WLC. Dit is van cruciaal belang tijdens de ontwerpfasen (ook voor probleemoplossing), aangezien al de RADIUS-verificatie en het boekhoudverkeer plaatsvinden tussen ISE en de externe WLC.
- Zodra de Redirect AVP's zijn toegepast op de clientsessie, werkt de Foreign WLC de clientsessie in het Anker bij via een mobiliteitshandoff-bericht.
- Op dit punt begint Anker WLC om Redirect af te dwingen met behulp van Redirect-ACL die vooraf is geconfigureerd.
- De accounting moet volledig worden uitgeschakeld op de Anchor WLC SSID om boekhoudkundige updates voor ISE (met dezelfde authenticatie-gebeurtenis als referentie) te voorkomen die zowel van het Anker als van Buitenlandse komen.
- Op URL gebaseerde ACL's worden niet ondersteund in buitenlandse ankerscenario's.

Problemen oplossen

Veelvoorkomende verbroken statussen op zowel AireOS als geconvergeerde access WLC

1. De client kan zich niet bij de gast-SSID aansluiten

Een "**show client detailleerde xx:xx:xx:xx:xx:xx**" onthult dat de client vastzit in **START**. Meestal is dit een indicator van de WLC die geen attribuut kan toepassen dat de AAA-server terugkeert.

Controleer dat de naam van de omgeleid ACL die door ISE wordt gedrukt, exact overeenkomt met de naam van de vooraf gedefinieerde ACL op de WLC.

Het zelfde principe is van toepassing op een ander attribuut dat u ISE hebt geconfigureerd om naar de WLC te gaan (VLAN-id's, interfacenamen, AirSpace-ACL's). De client moet dan overgaan naar DHCP en vervolgens **CENTRAL_WEB_AUTH**.

2. Redirect AVP's worden toegepast op de sessie van de klant, maar redirect werkt niet

Controleer of de beleidsbeheerderstatus van de client **CENTRAL_WEB_AUTH** is met een geldig IP-adres dat is uitgelijnd op de geconfigureerde dynamische interface voor de SSID en ook of de kenmerken Redirect ACL en URL-Redirect zijn toegepast op de sessie van de client.

ACL-omleiding

In AireOS WLCs moet de omleiden ACL expliciet het verkeer dat niet moet worden omgeleid, zoals DNS en ISE op TCP-poort 8443 in beide richtingen en de impliciete ontkenningen op elke triggers de rest van het verkeer om te worden omgeleid.

In geconvergeerde toegang is de logica het tegenovergestelde. Ontken ACE's omleidingen omleiden terwijl de vergunning ACE's de omleiding teweegbrengt. Dit is waarom het wordt aanbevolen om TCP poort 80 en 443 expliciet toe te staan.

Controleer de toegang tot ISE via poort 8443 van guest VLAN. Als alles er goed uitziet vanuit het configuratieperspectief is de gemakkelijkste manier om vooruit te gaan een opname achter de draadloze adapter van de client te pakken en te controleren waar de doorverwijzing onderbreekt.

- Is DNS-oplossing mogelijk?
- Is TCP 3 way handshake voltooid tegen de gevraagde pagina?
- Keert de WLC een redirect actie terug nadat de klant de GET heeft geïnitieerd?
- Is de TCP 3 way handshake tegen ISE over 8443 voltooid?

3. De client heeft geen toegang tot het netwerk nadat ISE een VLAN-wijziging heeft doorgedrukt aan het einde van de gaststroom

Zodra de client een IP-adres aan het begin van de stroom heeft ingepakt (Pre Redirect status), als een VLAN-wijziging wordt ingedrukt nadat de Gast-verificatie gebeurt (post CoA opnieuw authenticeren), is de enige manier om een DHCP-release / vernieuwen in de Gaststroom (zonder postuur-agent) te dwingen door een java-applet die in mobiele apparaten niet werkt.

Hierdoor blijft de client zwart-gegrepen in VLAN X met een IP-adres van VLAN Y. Hiermee moet rekening worden gehouden bij de planning van de oplossing.

4. ISE toont "HTTP 500 Interne fout, Radius sessie niet gevonden" bericht in de browser van de gast client tijdens omleiden

Dit is gewoonlijk een indicator van zittingsverlies op ISE (de zitting is geëindigd). De meest voorkomende reden hiervoor is de accounting geconfigureerd op de Anker WLC wanneer Foreign-Anchor is geïmplementeerd. Om dit te repareren schakelt accounting uit op het anker en laat de Foreign handle verificatie en accounting.

5. De cliënt maakt en blijft losgemaakt of verbindt met een verschillende SSID na het goedkeuren van AUP in het portaal van ISEHotSpot.

Dit kan worden verwacht in HotSpot vanwege de Dynamic Change of Authorisation (CoA) betrokken bij deze stroom (CoA Admin Reset) die ervoor zorgt dat de WLC een deauth aan het draadloze station geeft. De meerderheid van draadloze endpoints heeft geen problemen om terug te komen naar de SSID nadat de-authenticate gebeurt, maar in sommige gevallen verbindt de client zich met een andere voorkeursSSID in reactie op de gedeconstrueerde gebeurtenis. Niets kan van ISE of WLC worden gedaan om dit te voorkomen aangezien het aan de draadloze client is om aan de oorspronkelijke SSID te blijven plakken of verbinding te maken met een andere beschikbare (voorkeurs) SSID.

In dit geval moet de draadloze gebruiker handmatig opnieuw verbinding maken met de HotSpot SSID.

AireOS WLC

```
(Cisco Controller) >debug client
```

Debug client sets om te DEBUG een set van componenten betrokken bij client state machine veranderingen.

```
(Cisco Controller) >show debug
```

```
MAC Addr 1..... AA:AA:AA:AA:AA:AA
```

```
Debug Flags Enabled:
```

```
  dhcp packet enabled.  
  dot11 mobile enabled.  
  dot11 state enabled  
  dot1x events enabled.  
  dot1x states enabled.  
  mobility client handoff enabled.  
  pem events enabled.  
  pem state enabled.  
  802.11r event debug enabled.  
  802.11w event debug enabled.  
  CCKM client debug enabled.
```

Debug AAA-componenten

```
(Cisco Controller) >debug aaa {events, detail and packets} enable
```

Dit kan van invloed zijn op bronnen, afhankelijk van de hoeveelheid gebruikers die verbinding maken via MAB of Dot1X SSID. Deze componenten in DEBUG level registreren AAA transacties tussen WLC en ISE en drukken de RADIUS pakketten op het scherm.

Dit is cruciaal als u dat ISE niet de verwachte eigenschappen kan leveren, of als de WLC ze niet correct verwerkt.

Web-autorisatie omleiden

```
(Cisco Controller) >debug web-auth redirect enable mac aa:aa:aa:aa:aa:aa
```

Dit kan worden gebruikt om te verifiëren dat WLC met succes redirect activeert. Dit is een voorbeeld van hoe redirect moet eruit zien van debugs:

```
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser host is 10.10.10.10  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- parser path is /  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- added redirect=, URL is now  
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44  
212-2da2-11e6-a5e2-005056a15f11&action=cwa&to  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- str1 is now  
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44  
212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20c  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- clen string is Content-Length: 430  
  
*webauthRedirect: Jul 07 19:18:08.035: 68:7f:74:72:18:2e- Message to be sent is  
HTTP/1.1 200 OK  
Location:  
https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44  
212-2da2-11e6-a5e2-0050
```


Debug client sets om te DEBUG een set van componenten betrokken bij client state machine veranderingen.

```
3850#debug client mac-address <client MAC>
```

Deze component drukt de RADIUS-pakketten (verificatie en accounting) op het scherm af. Dit is handig wanneer u moet verifiëren dat ISE de juiste AVP's levert en ook om te verifiëren dat CoA wordt verzonden en correct verwerkt.

```
3850#debug radius
```

Dit zal alle AAA-overgangen (verificatie, autorisatie en accounting) waarbij draadloze clients betrokken zijn. Dit is van cruciaal belang om te verifiëren dat WLC de AVP's correct parseert en deze op de clientsessie toepast.

```
3850#debug aaa wireless all
```

Dit kan worden ingeschakeld wanneer u een omleidingsprobleem op de NGWC vermoedt.

```
3850#debug epm plugin redirect all
3850#debug ip http transactions
3850#debug ip http url
```

ISE

RADIUS live logs

Controleer of het eerste MAB-verzoek correct is verwerkt in ISE en dat ISE de verwachte kenmerken tegenhoudt. Navigeer naar **Operations > RADIUS > Live logs** en filter de uitvoer met de client-MAC onder **Endpoint ID**. Zodra de verificatiegebeurtenis is gevonden, klikt u op details en verifieert u de resultaten die als onderdeel van de acceptatie worden gedrukt.

The screenshot shows the ISE RADIUS Live Logs interface. At the top, there is a navigation bar with the date 'Jul ...', a search icon, and several filters: '68:7F:74:72:18:2E', '68:7F:74:72:18:2E', 'GuestSSO_Portal', and 'Cisco_5508'. Below the navigation bar, the 'Result' section is displayed. It contains a table with the following entries:

UserName	68:7F:74:72:18:2E
User-Name	68-7F-74-72-18-2E
State	ReauthSession:0e249a0500000682577ee2a2
Class	CACS:0e249a0500000682577ee2a2:TORISE21A/254695377/6120
cisco-av-pair	url-redirect-acl=TOR_Redirect
cisco-av-pair	url-redirect=https://TORISE21A.RTPAAA.NET:8443/portal/gateway?sessionId=0e249a0500000682577ee2a2&portal=9fc44212-2da2-11e6-a5e2-005056a15f11&action=cwa&token=c455b075d20cf2b4e969abb648533fea

TCP-Dump

Deze eigenschap kan worden gebruikt wanneer een diepere blik in de het pakketuitwisseling van de RADIUS tussen ISE en WLC nodig is. Op deze manier kunt u bewijzen dat ISE de juiste attributen in de access-accept verstuurt zonder dat debugs aan de WLC-kant moeten worden ingeschakeld. Om een opname te starten met TCDDump, navigeer naar **Operations > Probleemoplossing > Diagnostische tools > Algemene tools > TCPDump**.

Dit is een voorbeeld van een correcte stroom die door TCPDump is opgenomen

Source	Destination	Protocol	Length	Info
████████.154.5	████████.157.13	RADIUS	299	Access-Request(1) (id=0, l=257)
████████.157.13	████████.154.5	RADIUS	443	Access-Accept(2) (id=0, l=401)
████████.154.5	████████.157.13	RADIUS	340	Accounting-Request(4) (id=8, l=298)
████████.157.13	████████.154.5	RADIUS	62	Accounting-Response(5) (id=8, l=20)
████████.157.13	████████.154.5	RADIUS	244	CoA-Request(43) (id=1, l=202)
████████.154.5	████████.157.13	RADIUS	80	CoA-ACK(44) (id=1, l=38)
████████.154.5	████████.157.13	RADIUS	299	Access-Request(1) (id=1, l=257)
████████.157.13	████████.154.5	RADIUS	239	Access-Accept(2) (id=1, l=197)

Hier vindt u de AVP's die worden verstuurd in reactie op het initiële MAB-verzoek (tweede pakket in de screenshot hierboven).

RADIUS Protocol

Code: Access-Accept (2)

Packet identifier: 0x0 (0)

Length: 401

Authenticator: fleaaaffcfaa240270b885a9ba8ccd06d

[This is a response to a request in frame 1]

[Time from request: 0.214509000 seconds]

Attribute Value Pairs

AVP: l=19 t=User-Name(1): 00-05-4E-41-19-FC

AVP: l=40 t=State(24): 52656175746853657373696f6e3a30653234396130353030...

AVP: l=55 t=Class(25): 434143533a30653234396130353030303030616130353536...

AVP: l=37 t=Vendor-Specific(26) v=ciscoSystems(9)

VSA: l=31 t=Cisco-AVPair(1): url-redirect-acl=Gues_Redirect

AVP: l=195 t=Vendor-Specific(26) v=ciscoSystems(9)

VSA: l=189 t=Cisco-AVPair(1): url-

redirect=https://ise21a.rtpaaa.net:8443/portal/gateway?sessionId=0e249a0500000aa05565e1c9&portal=194a5780-5e4e-11e4-b905-005056bf2f0a&action=cwa&token=c6c8a6b0d683ea0c650282b4372a7622

AVP: l=35 t=Vendor-Specific(26) v=ciscoSystems(9)

Endpoint debugs:

Als u dieper in ISE-processen moet duiken die beleidsbeslissingen, poortselectie, gastverificatie, CoA-behandeling van de gemakkelijkste manier om dit te benaderen, is om **Endpoint Debugs** toe te laten in plaats van het moeten volledige componenten te bepalen om niveau te zuiveren.

Om dit in te schakelen, navigeer naar **Operations > Problemen oplossen > Diagnostische tools > Algemene tools > EndPoint Debug**.

Overview

Event	5200 Authentication succeeded
Username	00:24:97:BA:84:81
Endpoint Id	00:24:97:BA:84:81 ⓘ Endpoint Debug...
Endpoint Profile	Cisco-Device
Authentication Policy	Default >> MAB >> Default
Authorization Policy	Default >> Wireless_CWA_RedirectSSO
Authorization Result	GuestSSO_Portal

Enmaal in de Endpoint debug pagina, voer het eindpunt MAC-adres in en klik op Start wanneer u klaar bent om het probleem opnieuw te maken.

▼ General Tools

- RADIUS Authentication Trouble...
- Execute Network Device Com...
- Evaluate Configuration Validator
- Posture Troubleshooting
- EndPoint Debug
- TCP Dump

Endpoint Debug


Status: ⊘ Stopped Start


MAC Address IP ⓘ


Automatic disable after Minutes ⓘ

Zodra debug is tegengehouden klik op de link die de endpoint ID identificeert om de debug uitvoer te downloaden.

Endpoint Debug

Status:  Processing ...

MAC Address IP 

Automatic disable after Minutes 

Selected 0 | Total 1

<input type="checkbox"/>	File Name	Host Name	Modified Date	Size (Bytes)
<input type="checkbox"/>	68-7f-74-72-18-2e	TORISE21A	Jul 8 12:06	1021448

Gerelateerde informatie

[Door TAC aanbevolen AireOS-builds](#)

[Configuratiehandleiding voor Cisco draadloze controllers, release 8.0.](#)

[Beheerdershandleiding voor Cisco Identity Services Engine, release 2.1](#)

[Universele NGWIC draadloze configuratie met Identity Services Engine](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.