

Configuratievoorbeeld voor Identity Services Engine Guest

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[LWA-proces met ISE Guest Portal](#)

[Netwerkdigram](#)

[Configuratievoorwaarden](#)

[De WLC configureren](#)

[Configureer externe ISE als wereldwijde webauth URL](#)

[Het configureren van de toegangscontrolelijsten \(ACL's\)](#)

[Configureer de Service Set-id \(SSID\) voor LWA](#)

[De ISE configureren](#)

[Het netwerkapparaat definiëren](#)

[Het verificatiebeleid configureren](#)

[Het machtigingsbeleid en de resultaten configureren](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u Lokale Web Verificatie (LWA) kunt configureren met het Cisco Identity Services Engine (ISE) gastartaal.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE
- Cisco draadloze LAN-controller (WLC)

Gebruikte componenten

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

- ISE versie 1.4
- WLC versie 7.4

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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

In dit document wordt de configuratie van de LWA beschreven. Echter, Cisco raadt u aan om Gecentraliseerde Web Verificatie (CWA) met ISE te gebruiken wanneer mogelijk. Er zijn een paar scenario's waar LWA de voorkeur heeft of de enige optie, dus dit is een configuratievoorbeeld voor die scenario's.

Configureren

Voor LWA zijn bepaalde vereisten en een grote configuratie op de WLC vereist, evenals een aantal wijzigingen die op de ISE nodig zijn.

Voordat deze worden behandeld, is hier een overzicht van het LWA-proces met de ISE.

LWA-proces met ISE Guest Portal

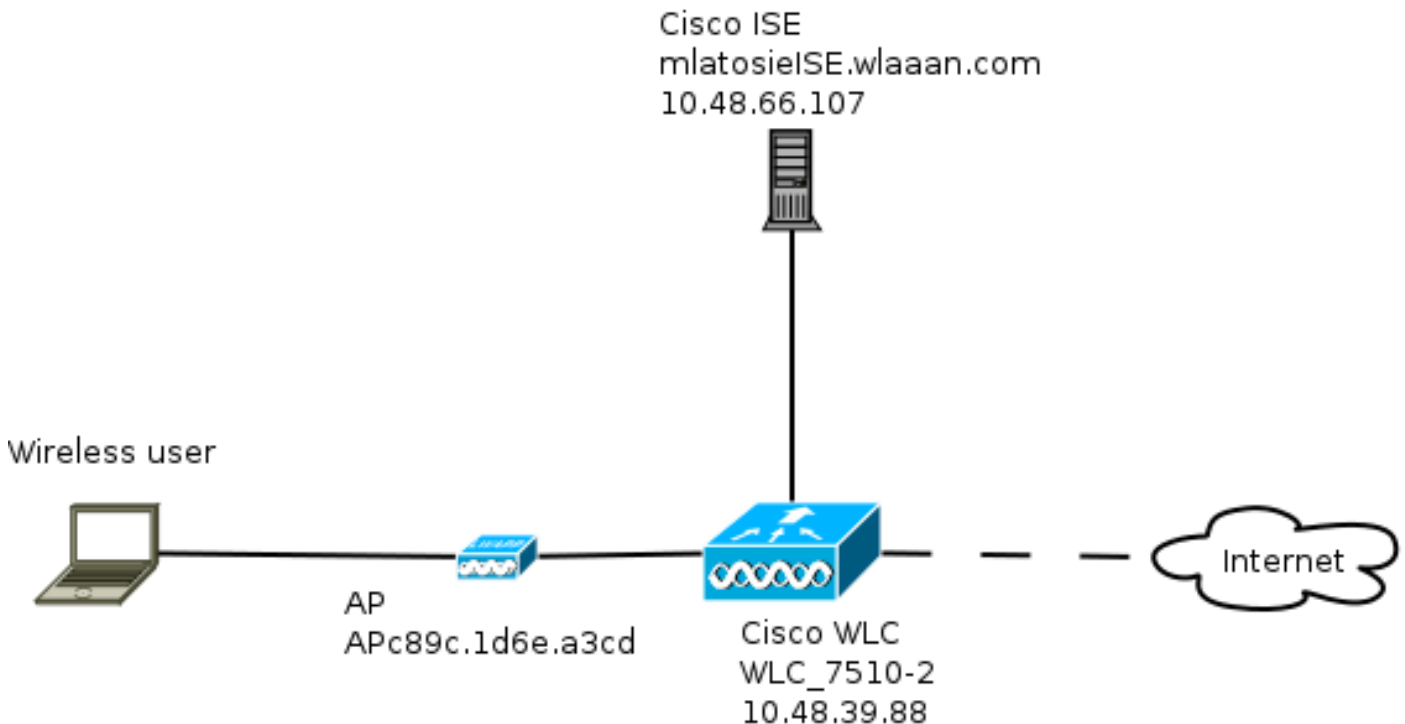
1. De browser probeert een webpagina te vinden.
2. De WLC onderscheppt het HTTP(S)-verzoek en stuurt het terug naar de ISE. Verschillende belangrijke stukken informatie worden opgeslagen in die HTTP redirect header. Hier is een voorbeeld van de URL-omleiding:
https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9#&ui-state=dialog?switch_url=https://1.1.1.1/login.html&ap_mac=b8:be:bf:14:41:90&client_mac=28:cf:e9:13:47:cb&wlan=mlatosie_LWA&redirect=yahoo.com/
 Vanuit de voorbeeld-URL, kunt u zien dat de gebruiker "yahoo.com" probeerde te bereiken. De URL bevat ook informatie over de Wireless Local Area Network (WLAN) naam (behalve externe LAN) en de client- en toegangspoint (AP) MAC-adressen. In het voorbeeld URL, is **1.1.1.1** de WLC, en **mlatosieise.wlaaan.com** is de ISE server.
3. De gebruiker wordt met de inlogpagina van de ISE-gast weergegeven en geeft de gebruikersnaam en het wachtwoord in.
4. ISE voert authenticatie uit tegen de geconfigureerde identiteitsvolgorde.
5. De browser richt zich opnieuw. In dit geval geeft het aanmeldingsgegevens aan de WLC door. De browser geeft de gebruikersnaam en het wachtwoord die de gebruiker in ISE heeft ingevoerd zonder extra interactie van de gebruiker. Hier is een voorbeeld: KRIJG verzoek aan de WLC.
 GET
[/login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0](http://login.html?redirect_url=http://yahoo.com/&username=mlatosie%40cisco.com&password=ityh&buttonClicked=4&err_flag=0)
 Opnieuw zijn de oorspronkelijke URL (**yahoo.com**), de gebruikersnaam (**mlatosie@cisco.com**) en het wachtwoord (**ityh**) inbegrepen.

Opmerking: Hoewel de URL hier zichtbaar is, wordt het eigenlijke verzoek ingediend via Secure Socket Layer (SSL), dat door HTTPS wordt aangegeven, en moeilijk te onderscheppen is.

6. WLC gebruikt RADIUS om die gebruikersnaam en wachtwoord voor ISE te authenticeren en geeft toegang tot deze applicatie.
7. De gebruiker wordt naar het aangegeven portal verwezen. Raadpleeg de sectie "**Externe ISE configureren als de webauth URL**" van dit document voor meer informatie.

Netwerkdigram

Dit getal beschrijft de logische topologie van apparaten die in dit voorbeeld worden gebruikt.



Configuratievoorwaarden

Om het LWA-proces naar behoren te laten functioneren, moet een cliënt de volgende informatie kunnen verkrijgen:

- IP-adres en netwerkmaskerconfiguratie
- Standaardroute
- Domain Name System (DNS)-server

Deze kunnen allemaal met DHCP of de lokale configuratie worden geleverd. De DNS-resolutie moet correct werken om de LWA te kunnen laten werken.

De WLC configureren

Configureer externe ISE als wereldwijde webauth URL

Onder **Security > Web Auth > Web Login Page** kunt u deze informatie bekijken.

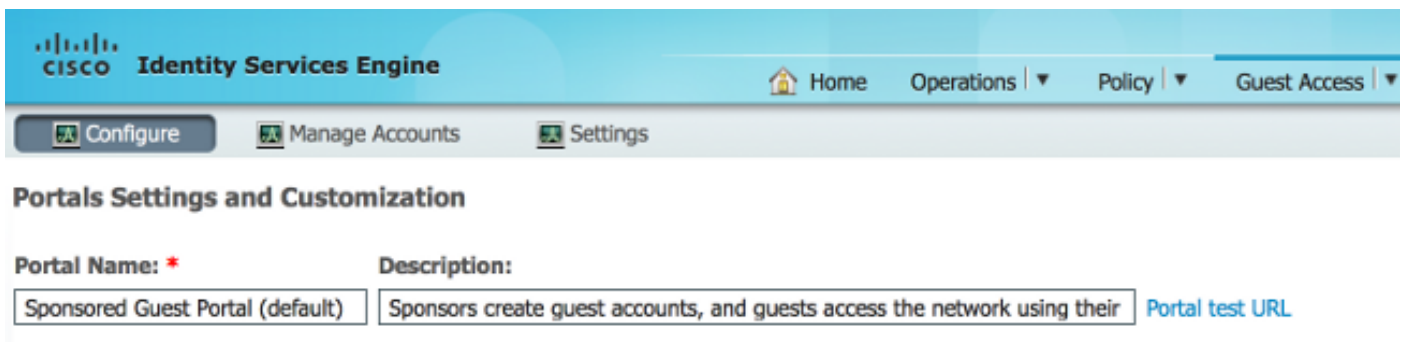
Web Login Page

Web Authentication Type	External (Redirect to external server) 
Redirect URL after login	<input type="text"/>
External Webauth URL	<input type="text" value="https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=2"/>

Opmerking: Dit voorbeeld gebruikt een Externe Webauth URL en is afkomstig van ISE versie 1.4. Als u een andere versie hebt, raadpleeg de configuratiegids om te begrijpen wat er moet worden geconfigureerd.

Het is ook mogelijk om deze instelling per-WLAN te configureren. Het bevindt zich vervolgens in de specifieke WLAN-beveiligingsinstellingen. Die overstijgen de mondiale omgeving.

Om de juiste URL voor uw specifieke portal te vinden, kiest u **ISE > Guest Policy > Configureer > uw specifieke portal**. Klik met de rechtermuisknop op de link van "portal test URL" en kies **kopieer link locatie**.



Portals Settings and Customization

Portal Name: * Description: [Portal test URL](#)

In dit voorbeeld is de volledige URL:

<https://mlatosieise.wlaaan.com:8443/portal/PortalSetup.action?portal=27963fb0-e96e-11e4-a30a-005056bf01c9>

Het configureren van de toegangscontrolelijsten (ACL's)

Voor web authenticatie om te werken, moet het toegestane verkeer worden gedefinieerd. Bepaal of FlexConnect ACL's of normale ACL's moeten worden gebruikt. FlexConnect APs gebruikt FlexConnect ACL's, terwijl APs die gecentraliseerde switching gebruiken normale ACL's gebruiken.

Om te begrijpen in welke modus een bepaalde AP werkt, kiest u **Draadloos > access points** en kiest u de **AP naam > AP Mode** vervolkeuzelijst. Een typische implementatie is of **lokaal of FlexConnect**.

Onder **Security > Access Control Lists** kiest u **FlexConnect ACL's** of **ACL's**. In dit voorbeeld is al het UDP-verkeer toegestaan om DNS-uitwisseling en -verkeer naar de ISE (10.48.66.107) specifiek toe te staan.

General

Access List Name FLEX_GUEST

Deny Counters 634752

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	Any	Any	Any	208398	<input checked="" type="checkbox"/>
2	Permit	10.48.66.107 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	Any	Any	Any	Any	32155	<input checked="" type="checkbox"/>
3	Permit	0.0.0.0 / 0.0.0.0	10.48.66.107 / 255.255.255.255	TCP	Any	Any	Any	Any	24532	<input checked="" type="checkbox"/>

Dit voorbeeld gebruikt FlexConnect, zodat **zowel** FlexConnect als standaard ACL's worden gedefinieerd.

Dit gedrag is gedocumenteerd in Cisco Bug ID [CSCue68065](#) met betrekking tot de WLC 7.4-controllers. Het is niet meer vereist op WLC 7.5 waar u alleen een FlexACL nodig hebt en geen standaard meer

Configureer de Service Set-id (SSID) voor LWA

Kies onder **WLAN's** de **WLAN-id** die moet worden bewerkt.

Configuratie webauteur

Pas dezelfde ACL's toe die in de vorige stap zijn gedefinieerd en maakt internetverificatie mogelijk.

WLANs > Edit 'mlatosie_LWA'

General Security QoS Advanced

Layer 2 Layer 3 AAA Servers

Layer 3 Security None ▾

Web Policy

Authentication

Passthrough

Conditional Web Redirect

Splash Page Web Redirect

On MAC Filter failure¹⁰

Preauthentication ACL IPv4 FLEX_GUEST ▾ IPv6 None ▾ WebAuth FlexAcl FLEX_GUEST ▾

Over-ride Global Config Enable

Opmerking: Als de lokale switchfunctie van FlexConnect wordt gebruikt, moet ACL-mapping op het AP-niveau worden toegevoegd. Dit kan worden gevonden onder **Draadloos > access points**. Kies de juiste **AP Naam > FlexConnect > Externe WebVerificatie ACL's**.

All APs > APc89c.1d6e.a3cd > ACL Mappings

AP Name APc89c.1d6e.a3cd
Base Radio MAC b8:be:bf:14:41:90

WLAN ACL Mapping

WLAN Id
WebAuth ACL

WLAN Id	WLAN Profile Name	WebAuth ACL
---------	-------------------	-------------

WebPolicies

WebPolicy ACL

WebPolicy Access Control Lists

Configuratie van verificatie, autorisatie en accounting (AAA) server

In dit voorbeeld wijzen zowel de authenticatie- als boekhoudservers naar de eerder gedefinieerde ISE-server.

General	Security	QoS	Advanced
Layer 2	Layer 3	AAA Servers	
Select AAA servers below to override use of default servers on this WLAN			
Radius Servers			
Radius Server Overwrite interface <input type="checkbox"/> Enabled			
		Authentication Servers	Accounting Servers
		<input checked="" type="checkbox"/> Enabled	<input checked="" type="checkbox"/> Enabled
Server 1		<input type="text" value="IP:10.48.66.107, Port:1812"/>	<input type="text" value="IP:10.48.66.107, Port:1813"/>

Opmerking: De standaardinstellingen onder het tabblad **Geavanceerd** hoeven niet te worden toegevoegd.

De ISE configureren

De ISE-configuratie bestaat uit meerdere stappen.

Eerst definieert u het apparaat als een netwerkapparaat.

Zorg er vervolgens voor dat de regels inzake echtheidscontrole en autorisatie voor deze uitwisseling bestaan.

Het netwerkapparaat definiëren

Onder **Beheer > Netwerkbronnen > Netwerkapparaten** vult u deze velden in:

- Apparaatnaam
- IP-adres apparaat
- **Verificatieinstellingen > Gedeeld geheim**

Network Devices

* Name
Description

* IP Address: /

Model Name
Software Version

* Network Device Group

WLC
Location
Device Type



Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

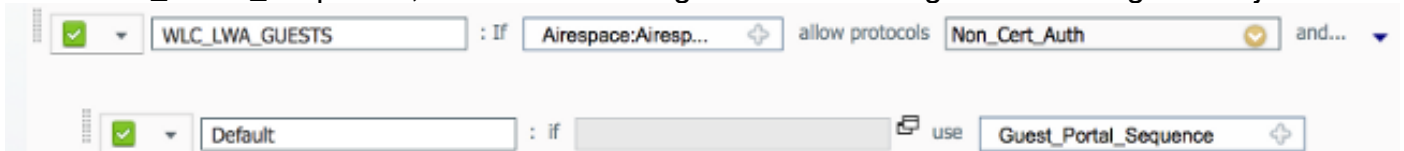
* Shared Secret

Het verificatiebeleid configureren

Onder **Policy > Verificatie**, voegt u een nieuw authenticatiebeleid toe.

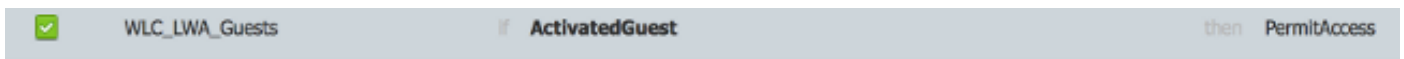
In dit voorbeeld worden deze parameters gebruikt:

- Name: **WLC_LWA_Guests**
- Voorwaardelijk: **Airespace:Airespace-WLAN-ID**. Deze voorwaarde komt overeen met de WLAN-id van 3, wat de ID is van de WLAN **matosie_LWA** die eerder op de WLC werd gedefinieerd.
- {optioneel} Het staat authenticatieprotocollen toe die niet het certificaat **Non_Cert_Auth** vereisen, maar de defaults kunnen worden gebruikt.
- **Guest_Portal_Sequence**, die definieert dat gebruikers lokaal gedefinieerde gasten zijn.



Het machtigingsbeleid en de resultaten configureren

Onder **Beleid > Toestemming**, definieer een nieuw beleid. Het kan een zeer fundamenteel beleid zijn, zoals:



Deze configuratie is afhankelijk van de algehele configuratie van de ISE. Dit voorbeeld wordt doelgericht vereenvoudigd.

Verifiëren

Op ISE kunnen beheerders live sessies controleren en probleemoplossing onder **Operations > Verificaties** controleren.

Er moeten twee authenticaties worden gezien. De eerste authenticatie komt uit het gastportaal op de ISE. De tweede authenticatie komt als een verzoek om toegang van de WLC tot de ISE.

May 15,13 02:04:02.589 PM	✓		mlatosie@cisco.com	WLC_7510-2	PermitAccess	ActivatedGuest	Authentication succeeded
May 15,13 02:03:59.819 PM	✓		mlatosie@cisco.com			ActivatedGuest	Guest Authentication Passed

U kunt op het pictogram **Verificatiegegevens** klikken om te controleren welk autorisatiebeleid en verificatiebeleid zijn gekozen.

Op de WLC kan een beheerder klanten onder **monitor > Clientbeheer** controleren.

Hier is een voorbeeld van een client die echt is geauthentiseerd:

28:cfe9:13:47:cb	APc89c.1d6e.a3cd	mlatosie_LWA	mlatosie_LWA	mlatosie@cisco.com	802.11bn	Associated	Yes	1	No
------------------	------------------	--------------	--------------	--------------------	----------	------------	-----	---	----

Problemen oplossen

Cisco raadt u aan debugs zo veel mogelijk via de client te gebruiken.

Via de CLI verschaffen deze uitvindingen nuttige informatie:


```
debug client MA:CA:DD:RE:SS
```

```
debug web-auth redirect enable macMA:CA:DD:RE:SS
```

```
debug aaa all enable
```

Gerelateerde informatie

- [Cisco ISE 1000x-configuratiegids](#)
- [Cisco WLC 700x-configuratiegids](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)