

Lichtgewicht access point instellen als een 802.1x applicator

Inleiding

Dit document beschrijft hoe u een lichtgewicht access point (LAP) kunt configureren als een 802.1x smeebede om authenticatie aan te vragen tegen de ISE-server (Identity Services Engine).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Draadloze LAN-controller (WLC) en LAP
- 802.1x op Cisco-switches
- ISE
- Uitbreidbaar verificatieprotocol (EAP) - Flexibele verificatie via Secure Tunneling (FAST)

Gebruikte componenten

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

- WS-C3560CX-8PC-S, 15.2(4)E1
- LUCHT-CT-2504-K9, 8.2.141.0
- ISE 2.0

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 deze instelling werkt het access point (AP) als de 802.1x-smeebede en is geauthentiseerd door de schakelaar tegen de ISE die EAP-FAST met anonieme Protected Access Credentials (PAC) voorziening gebruikt. Zodra de poort is ingesteld voor 802.1x-verificatie, staat de switch geen ander verkeer dan 802.1x-verkeer toe om door de poort te gaan totdat het apparaat dat is aangesloten op de poort authentiek verklaard heeft. AP kan of voor authentiek worden verklaard het zich bij een WLC aansluit of nadat het zich bij een WLC heeft aangesloten, in welk geval u 802.1x op de schakelaar vormt nadat de LAP zich bij WLC aansluit.

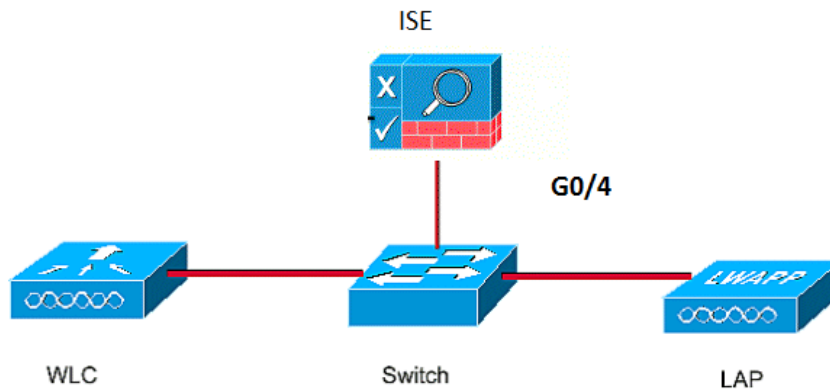
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden

beschreven.

Netwerkdigram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze IP-adressen:

- IP-adres van de switch is 10.48.39.141
- IP-adres van de ISE-server is 10.48.39.161
- IP-adres van de WLC is 10.48.39.142

De LAP configureren

In dit gedeelte wordt u met de informatie voorgesteld om de LAP als een 802.1x-smeekbede te configureren.

1. Als het AP al aangesloten is op WLC, ga het tabblad Draadloos en klik op het AP, ga het veld Credentials en onder de optie 802.1x Supplidiete Credentials, controleer het aanvinkvakje **Over-ride Global** geloofsbrieven om de gebruikersnaam en het wachtwoord voor dit AP in te stellen op 802.1x.

U kunt ook een gemeenschappelijke gebruikersnaam en wachtwoord instellen voor alle AP's die worden aangesloten op de WLC met behulp van het menu Global Configuration.

2. Als AP zich nog niet bij een WLC heeft aangesloten moet u in de LAP console troosten om de geloofsbriefen in te stellen en deze CLI opdrachten te gebruiken:

```
LAP#debug capwap console cli
LAP#capwap ap dot1x username
```

De switch configureren

1. Schakel dot1x mondiaal in op de schakelaar en voeg de ISE server aan de schakelaar toe.

```
aaa new-model
!  
aaa authentication dot1x default group radius
!  
dot1x system-auth-control
!  
radius server ISE
address ipv4 10.48.39.161 auth-port 1645 acct-port 1646
key 7 123A0C0411045D5679
```

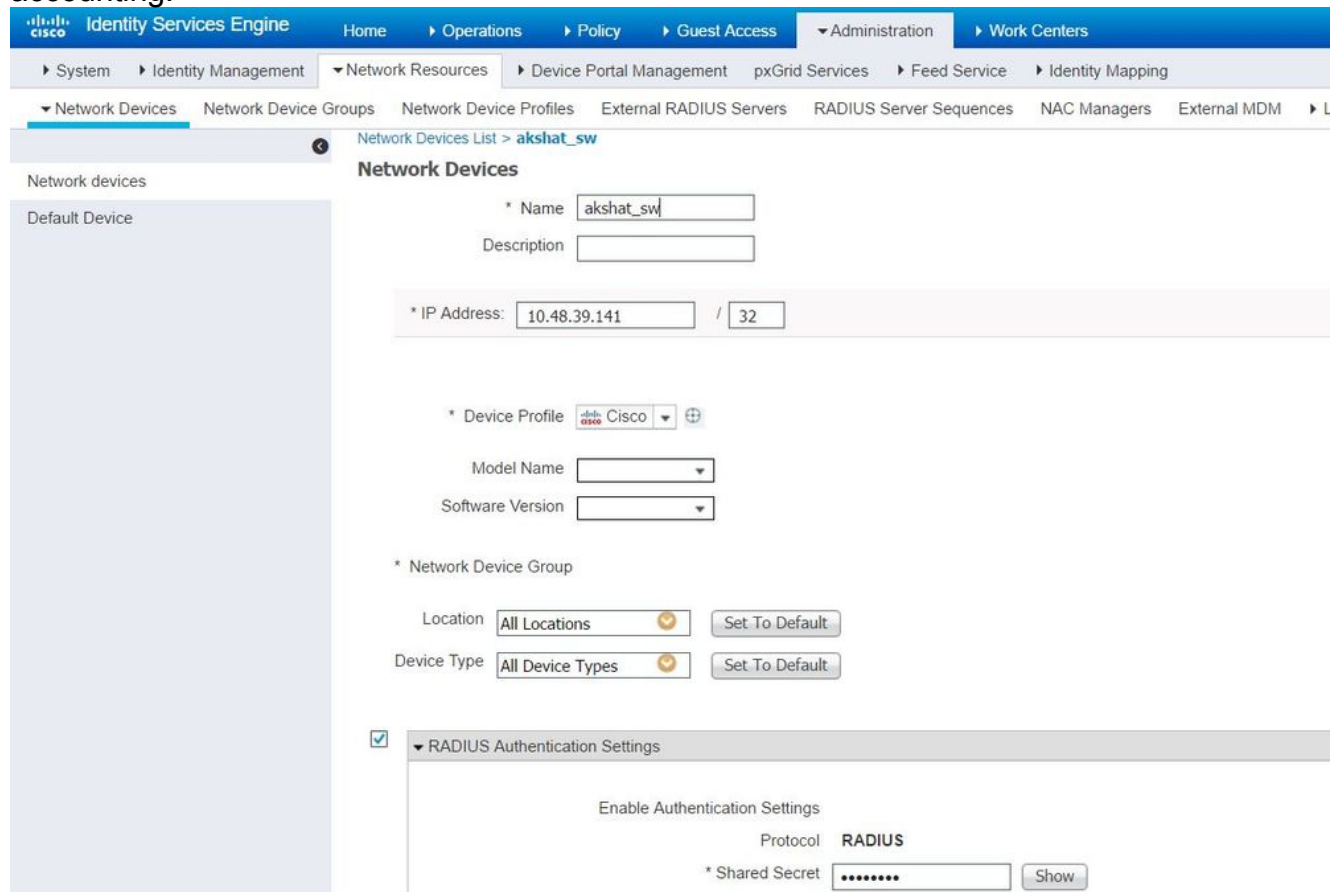
2. Stel nu de AP schakelaar poort in.

```
interface GigabitEthernet0/4
```

```
switchport access vlan 231
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
```

De ISE-server configureren

1. Voeg de switch toe als een AAA-client op de ISE-server. Verificatie, autorisatie en accounting.



The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface for a Network Device. The page is titled "Network Devices" and shows the configuration for a device named "akshat_sw".

The configuration fields are as follows:

- Name:** akshat_sw
- Description:** (empty)
- IP Address:** 10.48.39.141 / 32
- Device Profile:** Cisco
- Model Name:** (empty)
- Software Version:** (empty)
- Network Device Group:**
 - Location:** All Locations
 - Device Type:** All Device Types
- RADIUS Authentication Settings:**
 - Enable Authentication Settings:** (checked)
 - Protocol:** RADIUS
 - Shared Secret:** (masked with dots)

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location

Network devices

Default Device

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type
<input type="checkbox"/> GurpWLC1	10.48.39.155/32	Cisco	All Locations	All Device Types
<input type="checkbox"/> GurpWLC2	10.48.39.156/32	Cisco	All Locations	All Device Types
<input type="checkbox"/> akshat_sw	10.48.39.141/32	Cisco	All Locations	All Device Types

2. Op ISE, moet u het verificatiebeleid en het autorisatiebeleid configureren. In dit geval wordt de standaard authenticatieregel gebruikt die is aangesloten op punt 1.1x, maar je kunt de regel aanpassen aan de eisen.

Identity Services Engine Home Operations Policy Guest Access Administration Work

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity source. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If Wired_MAB OR
	Wireless_MAB	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use Internal Endpoints
<input checked="" type="checkbox"/>	Dot1X	: If Wired_802.1X OR
	Wireless_802.1X	Allow Protocols : Default Network Access and
<input checked="" type="checkbox"/>	Default	:use All_User_ID_Stores
<input checked="" type="checkbox"/>	Default Rule (If no match)	: Allow Protocols : Default Network Access and use : All_User_ID_Stores

Zorg ervoor dat in de toegestane protocollen dat de standaard toegang tot een netwerk is toegestaan.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Dictionarys Conditions Results

Authentication

Allowed Protocols

Authorization

Profiling

Posture

Client Provisioning

Allow EAP-FAST

EAP-FAST Inner Methods

Allow EAP-MS-CHAPv2

Allow Password Change Retries 3 (Valid Range 0 to 3)

Allow EAP-GTC

Allow Password Change Retries 3 (Valid Range 0 to 3)

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Use PACs Don't Use PACs

Tunnel PAC Time To Live 90 Days

Proactive PAC update will occur after 90 % of PAC Time To Live has expired

Allow Anonymous In-Band PAC Provisioning

Allow Authenticated In-Band PAC Provisioning

Server Returns Access Accept After Authenticated Provisioning

Accept Client Certificate For Provisioning

3. In dit geval zijn AP-referenties toegevoegd aan een gebruikersgroep (APs), wat betreft het autorisatiebeleid (Port_AuthZ). De gebruikte voorwaarde was "Als de gebruiker tot de groep AP behoort en de bekabelde punt1x doet, druk dan op de standaard Toestemming van het Profiel van de Vergunning toegang." Dit kan opnieuw worden aangepast aan de eisen.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

Authentication Authorization Profiling Posture Client Provisioning Policy Elements

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order. For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

First Matched Rule Applies

Exceptions (0)

Create a New Rule

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Port_AuthZ	if APs AND Wired_802.1X	then PermitAccess

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Identity Mapping

Identities Groups External Identity Sources Identity Source Sequences Settings

Identity Groups

User Identity Groups > APs

Identity Group

Name APs

Description Credentials for APs

Save Reset

Member Users

Users Selected 0 | Total 1

Add Delete Show All

Status	Email	Username	First Name	Last Name
✓ Enabled		ritmahaj		

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Als 802.1x op de switchpoort is ingeschakeld, wordt al het verkeer behalve het 802.1x-verkeer door de poort geblokkeerd. De LAP, die indien al bij de WLC geregistreerd, wordt niet aangesloten. Alleen na een succesvolle 802.1x-authenticatie is er nog ander verkeer dat mag doorgeven. Succesvolle registratie van de LAP naar de WLC nadat de 802.1x-schakelaar is ingeschakeld, geeft aan dat de LAP-verificatie succesvol is. U kunt deze methoden ook gebruiken om te controleren of het LAP echt is bevonden.

1. Voer in de schakelaar een van de opdrachten van de **show** in om te controleren of de poort al dan niet voor authentiek is verklaard.

```
akshat_sw#show dot1x interface g0/4
```

```
Dot1x Info for GigabitEthernet0/4
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

```
akshat_sw#show dot1x interface g0/4 details
```

```
Dot1x Info for GigabitEthernet0/4
-----
PAE = AUTHENTICATOR
QuietPeriod = 60
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 30
```

```
Dot1x Authenticator Client List
-----
EAP Method = FAST
Supplicant = 588d.0997.061d
Session ID = 0A30278D000000A088F1F604
Auth SM State = AUTHENTICATED
Auth BEND SM State = IDLE
```

```
akshat_sw#show authentication sessions
```

```
Interface MAC Address Method Domain Status Fg Session ID
Gi0/4 588d.0997.061d dot1x DATA Auth 0A30278D000000A088F1F604
```

2. In ISE, kies **Operations > Radius Livelogs** en zie dat de authenticatie succesvol is en dat het juiste autorisatieprofiel wordt geduwd.

Time	Status	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles
2017-03-09 10:32:28.956	All	1	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	PermitAccess
2017-03-09 10:31:29.227	All	1	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> Default	Default >> Port_AuthZ	PermitAccess

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

1. Voer de opdracht **ping in** om te controleren of de ISE-server bereikbaar is vanaf de schakelaar.
2. Zorg dat de switch als een AAA-client op de ISE-server is geconfigureerd.
3. Zorg ervoor dat het gedeelde geheim hetzelfde is tussen de schakelaar en de ACS server.
4. Controleer of EAP-FAST is ingeschakeld op de ISE-server.
5. Controleer of de 802.1x-referenties voor de LAP zijn ingesteld en op de ISE-server gelijk zijn.
Opmerking: De gebruikersnaam en het wachtwoord zijn hoofdlettergevoelig.
6. Als de authenticatie faalt, voer deze opdrachten in op de switch: **debug dot1x** en **debug authenticatie**.