CLOUD4WI – ALCATEL-LUCENT IAP CONFIGURATIE V2

Technote

Versie: 2.0
Auteur: Herwin de Rijke
Datum: 2-12-2014

Alcadis | Vleugelboot 8 | 3991 CL Houten | www.alcadis.nl | 030 – 65 85 125

Inhoud

1 Inleiding

In dit document wordt beschreven hoe u een Alcatel-Lucent Instant Access Point moet configureren om gebruik te maken van Cloud4Wi.

De instructies die in dit document gegeven worden gaan uit van een Engelstalige webinterface van het access point en eventuele Engelstalige documentatie. Mocht u de webinterface ingesteld hebben op de Nederlandse taal dan zullen de stappen hetzelfde zijn, maar de benaming van de menu's zullen verschillen.

De instructies die in dit document gegeven worden zijn op basis van firmwareversie 6.4.0.3-4.1.0.2_45704. Wij raden aan om uw access points te upgraden naar deze versie of hoger.

In dit document is ten opzichte van v1 een aanpassing gemaakt in de werking van de walled garden.

1.1 Doelstelling

De doelstelling van dit document is het bekend maken met de configuratie stappen voor het opzetten van een Cloud4Wi configuratie.

1.2 Beoogd publiek

Dit document is geschreven voor technisch personeel voor het maken van een koppeling tussen Cloud4Wi en de Alcatel-Lucent access points.

1.3 Voorkennis/Benodigdheden

Om optimaal te kunnen profiteren van wat er in dit document beschreven staat is het van belang dat u basiskennis heeft van de volgende onderwerpen:

- Alcatel-Lucent Webinterface

Om alle stappen goed te kunnen doorlopen heeft u minimaal de volgende hardware/software nodig:

- Alcatel-Lucent Instant Access Point
- Cloud4Wi Tenant Account

1.4 Extra informatie

Voor extra informatie over het configureren van de Cloud4Wi omgeving kunt u terecht op de website van Alcadis. Hier vind u technotes over hoe u de Cloud4Wi omgeving zelf kunt instellen. Denk hierbij aan bijvoorbeeld "**Access Template**", "**Splash Portal**" en de "**WiFi Area**".

2 AP Configuratie

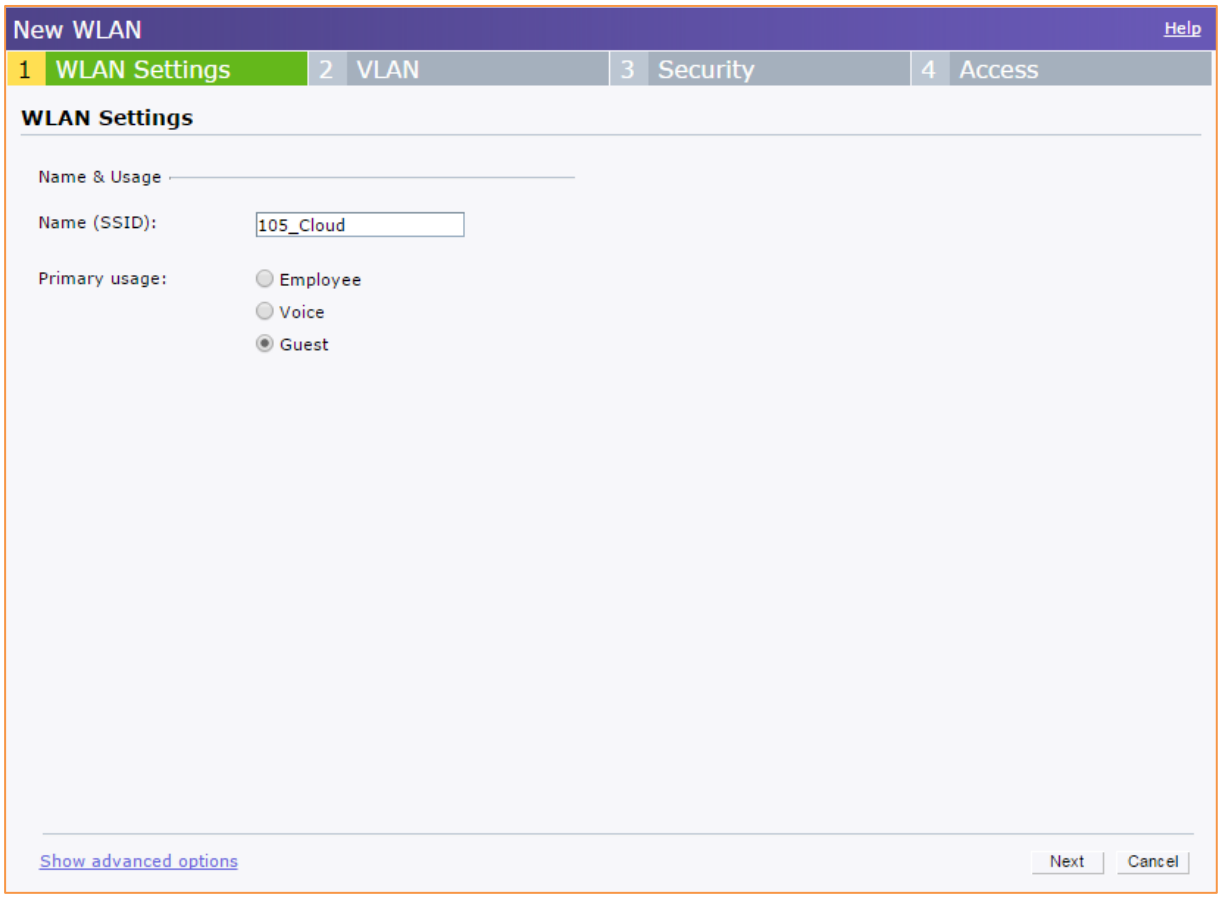
2.1 WLAN configuratie

Hieronder wordt beschreven hoe u een netwerk aanmaakt en deze configureert voor het gebruik van Cloud4Wi.

1. Login op de webinterface van het access point.
2. Klik op **"New"** onder "**Networks**" om een nieuw netwerk aan te maken.

Figuur 1: New Network

3. In het veld "**Name (SSID)**" geeft u dan naam op van het nieuwe Wi-Fi netwerk.
4. De optie "**Primary usage**" zet u op "**Guest**".
5. Klik op "**Next**" als u deze instellingen heeft gedaan.

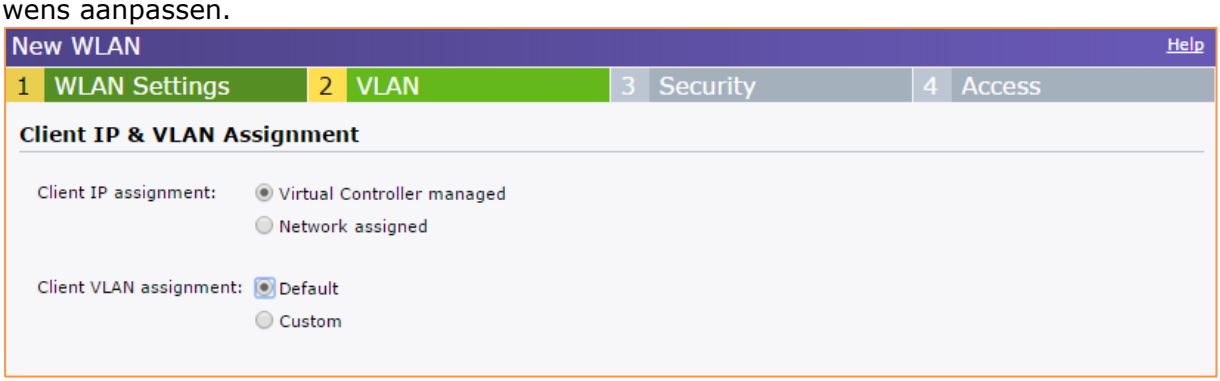


Figuur 2: WLAN Settings

6. De optie "**Client IP assignment**" kunt u op default laten staan.

7. De optie "**Client VLAN assignment**" kunt u ook op default laten staan.

Note: Mocht u gebruik willen maken van uw eigen DHCP server of wilt u een andere VLAN aan het netwerk koppelen dan kunt u de bovenstaande instellingen naar eigen wens aanpassen.

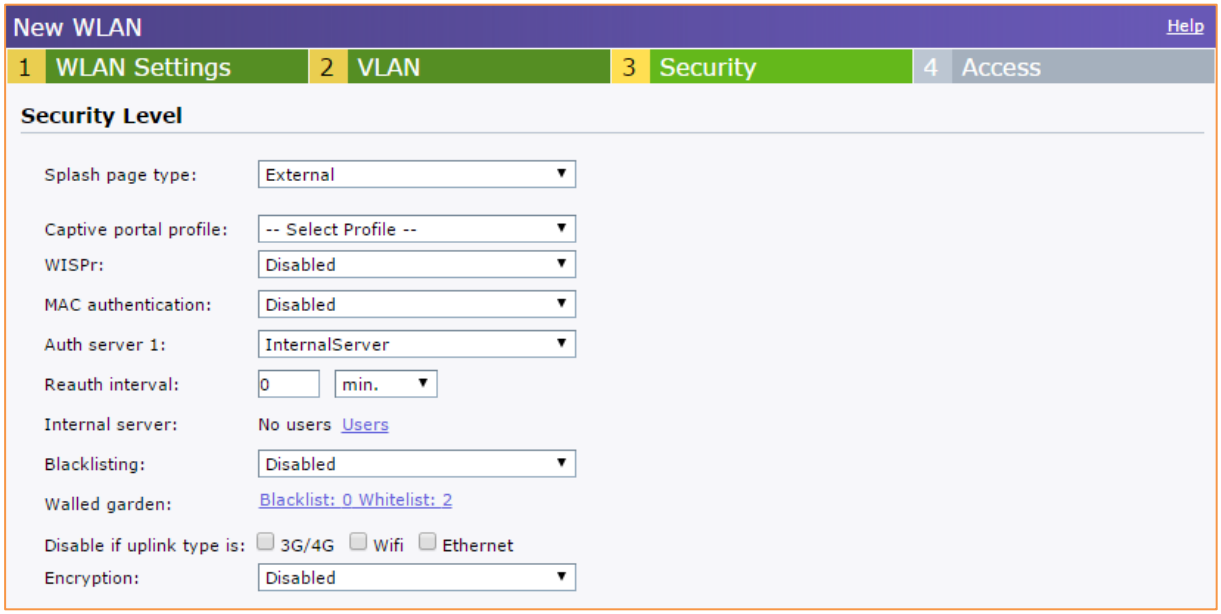


Figuur 3: VLAN Instellingen

8. De optie "**Splash page type**" zet u op "**External**".

9. De optie "**Captive portal profile**" zet u op "**New**", er opent nu een nieuw scherm voor het aanmaken van een nieuw captive portal profiel.

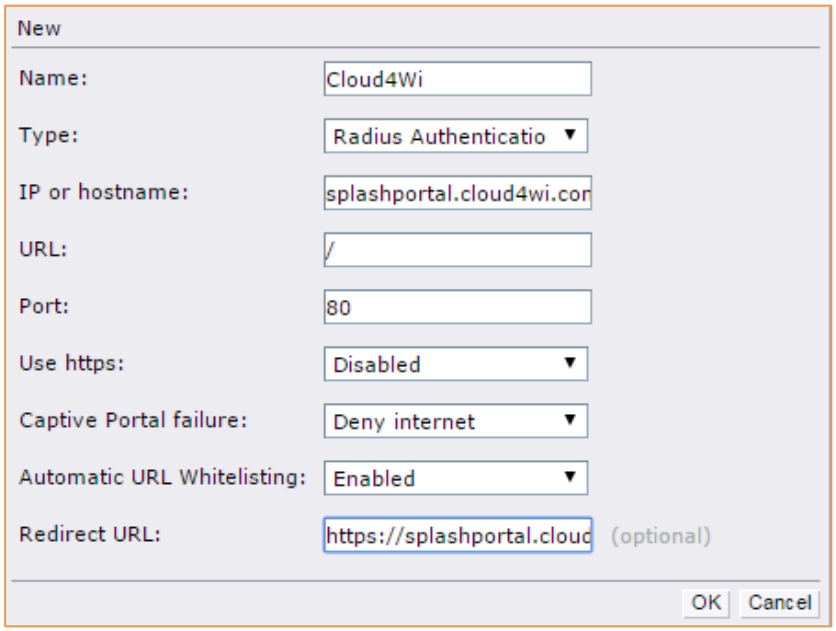
Note: Mocht u al eerder een Cloud4Wi profiel hebben aangemaakt dan kunt u hier het eerder aangemaakte Cloud4Wi profiel selecteren.



Figuur 4: Security Settings

In het geopende scherm kunt u de captive portal instellen.

1. In het veld "**Name:**" geeft u een naam op bijvoorbeeld: Cloud4Wi
2. De optie "**Type:**" zet u op Radius Authentication
3. In het veld "**IP or hostname**" vult u in: splashportal.cloud4wi.com
4. In het veld "**URL:**" vult u in: /
5. In het veld "**Port:**" vult u in: 80
6. De optie "**Use https:**" zet u op: Disabled
7. De optie "**Captive portal failure:**" zet u op: Deny Internet
8. De optie "**Automatic URL Whitelisting:**" zet u op: Enabled
9. In het veld "**Redirect URL:**" vult u in: https://splashportal.cloud4wi.com
10. Klik op "**OK**" om de wijzigingen op te slaan

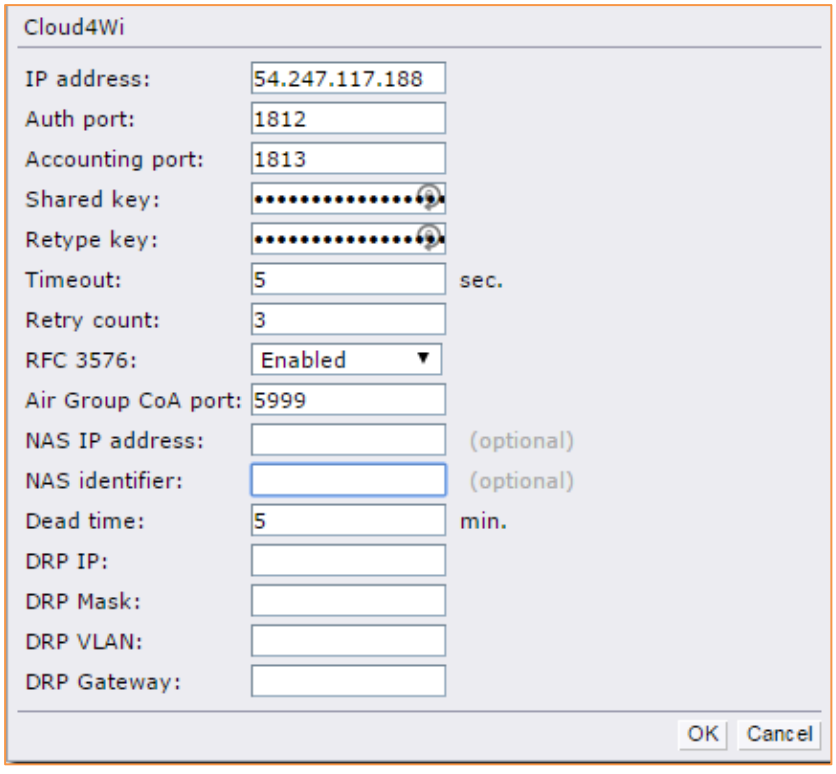


Figuur 5: Captive Portal Instellingen

In het scherm "**3 Security**" (Figuur 4) kiest u in het drop-down menu achter "**Auth server 1:**" voor "**New**". Er opent een venster waar u de instellingen voor de primaire radiusserver kunt configureren.

Note: Als u al eerder een Cloud4Wi radiusserver heeft geconfigureerd dan kunt u deze hier ook selecteren.

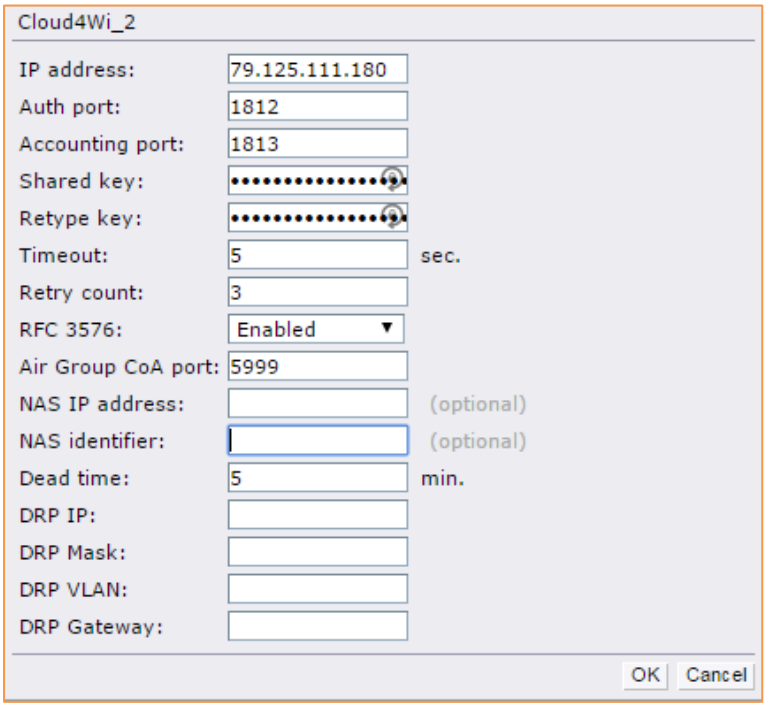
1. In het veld "**IP address**" vult u in: 54.247.117.188
2. In het veld "**Auth port**" vult u in: 1812
3. In het veld "**Accounting port:**" vult u in: 1813
4. In de velden "**Shared key:**" en "**Retype key:**" geeft u het secret op dat u van Alcadis heeft ontvangen
5. In de velden "**Timeout:**" en "**Retry count:**" kunt u de standaard waarden laten staan
6. De optie "**RFC 3576:**" zet u op Enabled
7. In het veld "**Air Group CoA port:**" vult u in: 5999
8. Alle overige velden kunt u op de standaard waarden laten staan
9. Klik op "**OK**" om de wijzigingen op te slaan



Figuur 6: Primaire Radiusserver

In het scherm "**3 Security**" (Figuur 4) kiest u in het drop-down menu achter "**Auth server 2:**" voor "**New**". Er opent een venster waar u de instellingen voor de secundaire radiusserver kunt configureren.

1. In het veld "**IP address**" vult u in: 79.125.111.180
2. In het veld "**Auth port**" vult u in: 1812
3. In het veld "**Accounting port:**" vult u in: 1813
4. In het veld "**Shared key:**" en "**Retype key:**" geeft u het secret op dat u van Alcadis heeft ontvangen
5. In de velden "**Timeout:**" en "**Retry count:**" kunt u de standaard waarden laten staan
6. De optie "**RFC 3576:**" zet u op Enabled
7. In het veld "**Air Group CoA port:**" vult u in: 5999
8. Alle overige velden kunt u op de standaard waarden laten staan
9. Klik op "**OK**" om de wijzigingen op te slaan.



Figuur 7: Secundaire radiusserver

Indien gewenst kunt u load balancing uit laten voeren tussen beide Radiusservers. U kiest dan in het scherm "**3 Security**" (Figuur 4) bij de optie "**Load Balancing**" voor "**Enabled**".

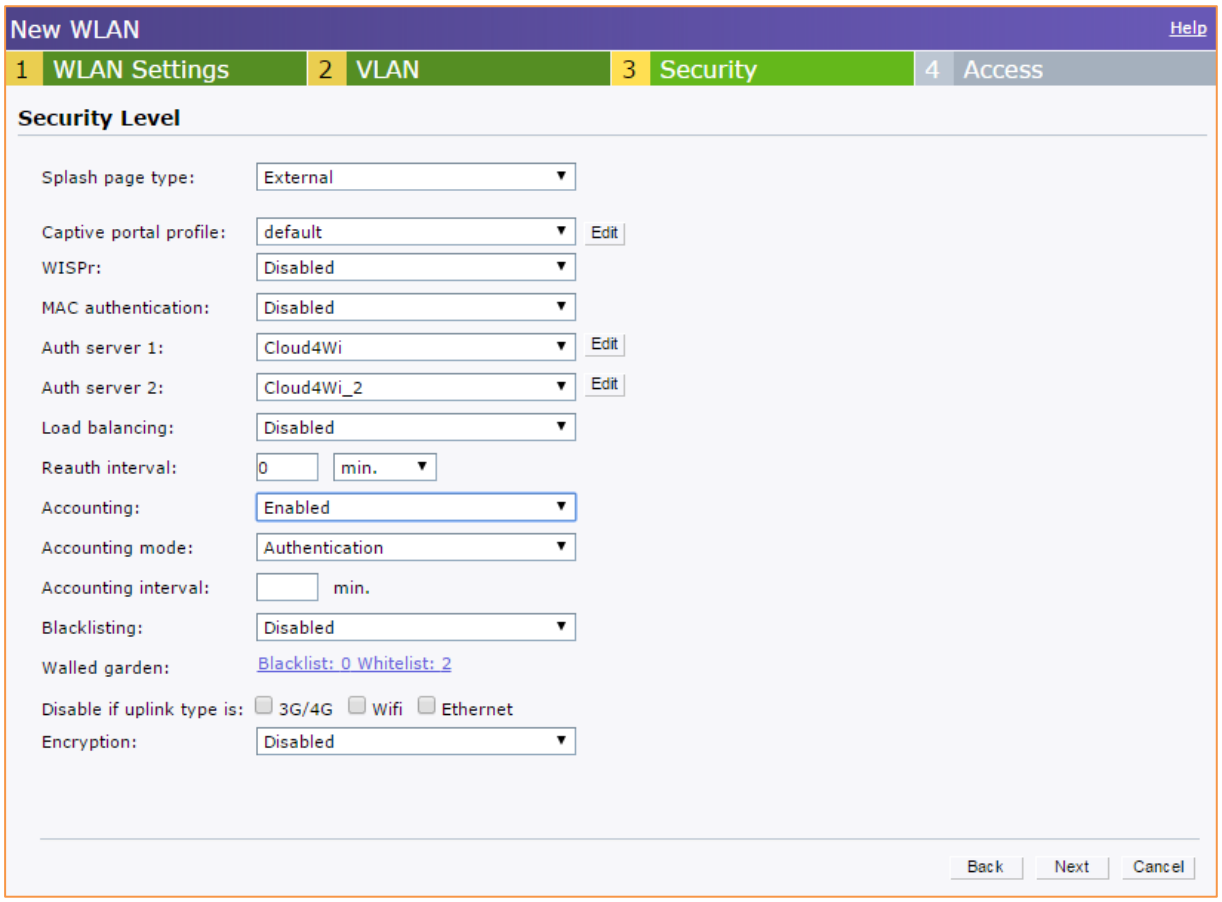
10. Zet de optie "**Accounting:**" op "**Enabled**".

11. Zet de optie "**Accounting mode:**" op "**Authentication**".

12. De overige instellingen kunnen op de standaard waarden blijven staan.

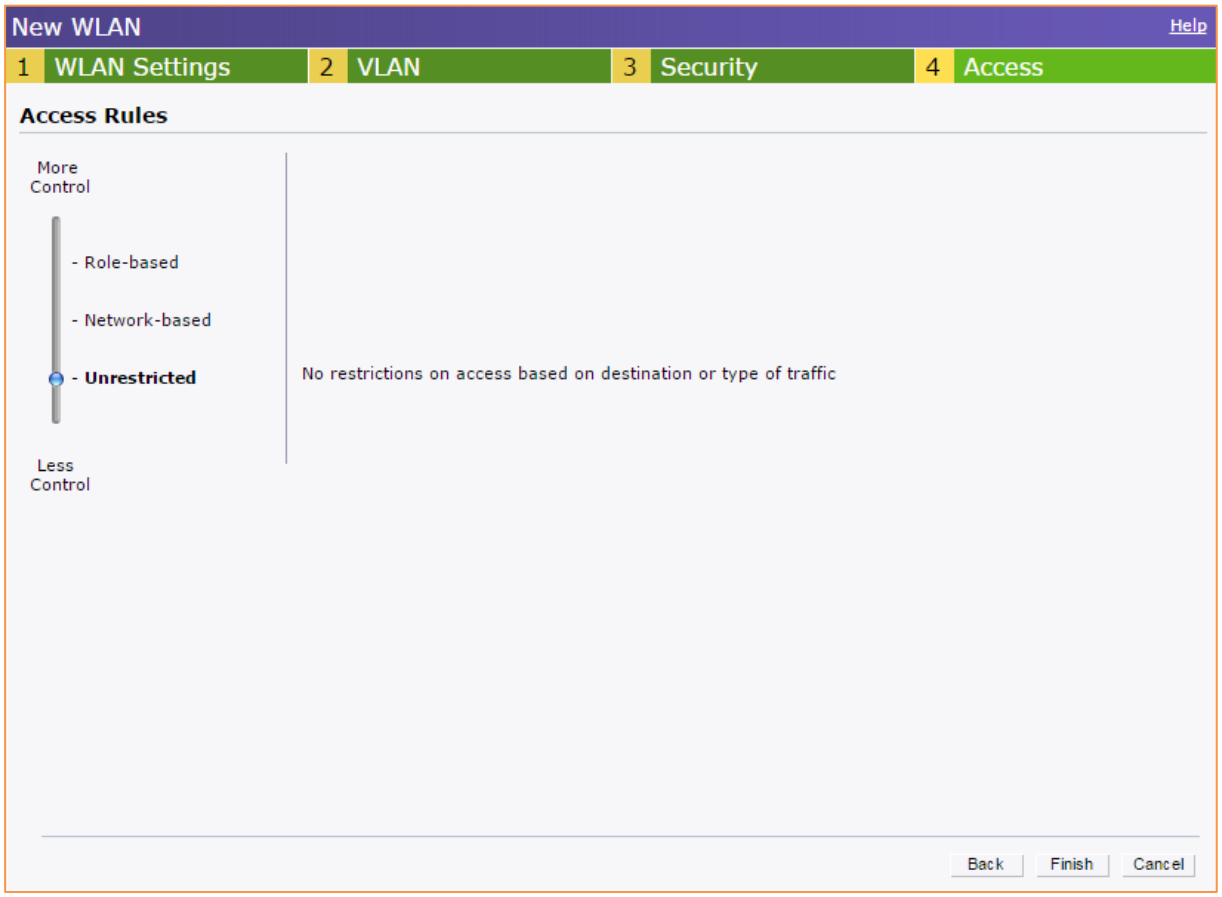
13. Als alle instellingen zijn gemaakt kunt u op "N**ext**" klikken om door te gaan.

Note: Eventueel kunt u in de "**Walled garden"** websites toevoegen die toegankelijk moeten blijven zonder dat mensen geauthentiseerd zijn via Cloud4Wi. Deze optie heeft u bijvoorbeeld nodig om authenticatie via Social login mogelijk te maken. Meer informatie hierover vind u in hoofdstuk 2.3 Walled Garden.



Figuur 8: Security Instellingen

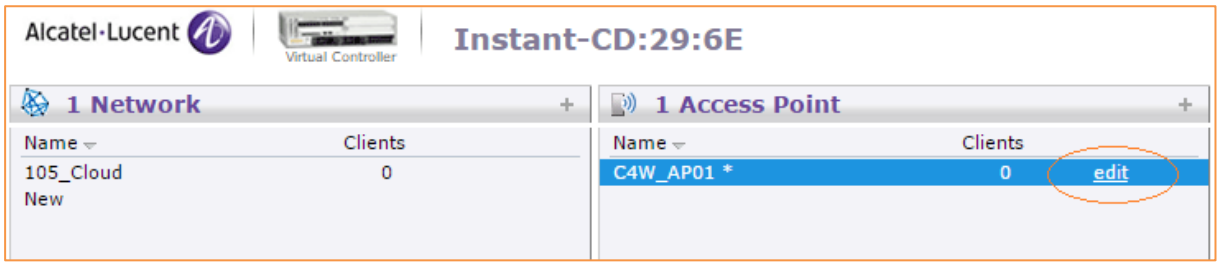
14. Op deze laatste pagina kunt u de toegang tot delen van het netwerk regelen. Als u geen gebruikt wil maken van social login mogelijkheden kunt u deze optie op **"unrestricted"** laten staan. Indien https pagina's in de walled garden een vereiste zijn, zoals voor social login moet u deze op **"Role-based"** zetten. In de paragraaf **"Role-based access"** wordt hier meer over uitgelegd.



Figuur 9: Access Instellingen

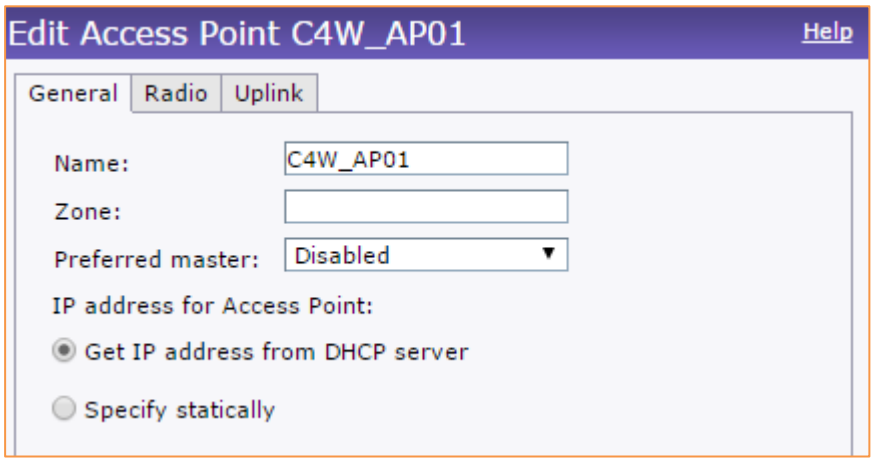
Het laatste wat u moet doen is de naam van het access point opzoeken. Deze naam stuurt het access point standaard mee als identifier.

15. Klik in de virtuele controller onder "**Access Point**" op "**Edit**".



Figuur 10: Virtuele Controller

In het scherm dat nu opent staat achter "**Name:**" de naam die als "**Identifier**" wordt meegestuurd. Om fouten te voorkomen kan het makkelijk zijn de naam van deze locatie te kopiëren.



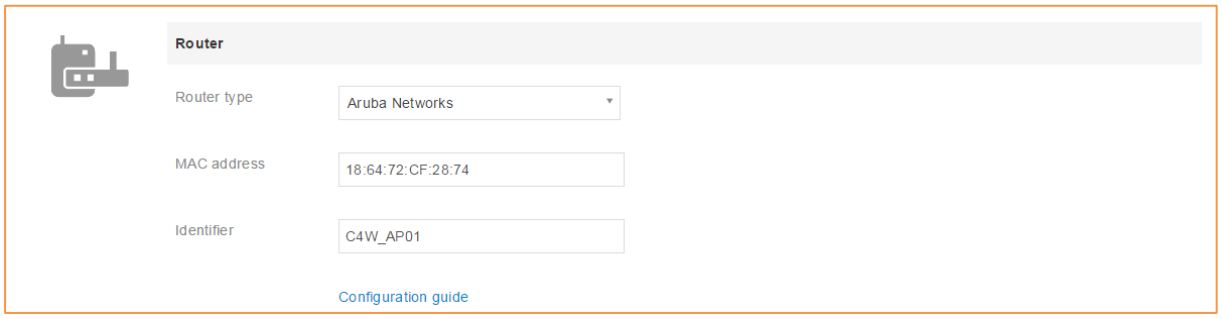
Figuur 11: Access Point

2.2 Cloud4Wi instellingen

Alle instellingen voor de Cloud4Wi omgeving kunt u vinden in diverse technotes op de support site van Alcadis. Alleen de specifieke Alcatel-Lucent instellingen zullen in deze paragraaf worden beschreven.

Als u bent ingelogd bij Cloud4Wi gaat u naar "**Hotspot**" in de betreffende "**WiFi Area**". Bij de instellingen voor de Hotspot kiest u bij Router voor de volgende instellingen:

1. De optie "**Router type**" zet u op: Aruba Networks
2. In het veld "**MAC address**" vult u in: <AP MAC-Adress>
3. In het veld "**Identifier**" vult u in: <AP-Naam>. Deze kunt u terugvinden via de webinterface van de virtuele controller.



Figuur 12: Cloud4Wi Hotspot

2.3 Walled Garden

De walled garden is bedoeld om gebruikers die nog niet zijn geauthentiseerd toch toegang te geven tot bepaalde websites. U kunt hier bijvoorbeeld de webpagina van uw bedrijf in zetten.

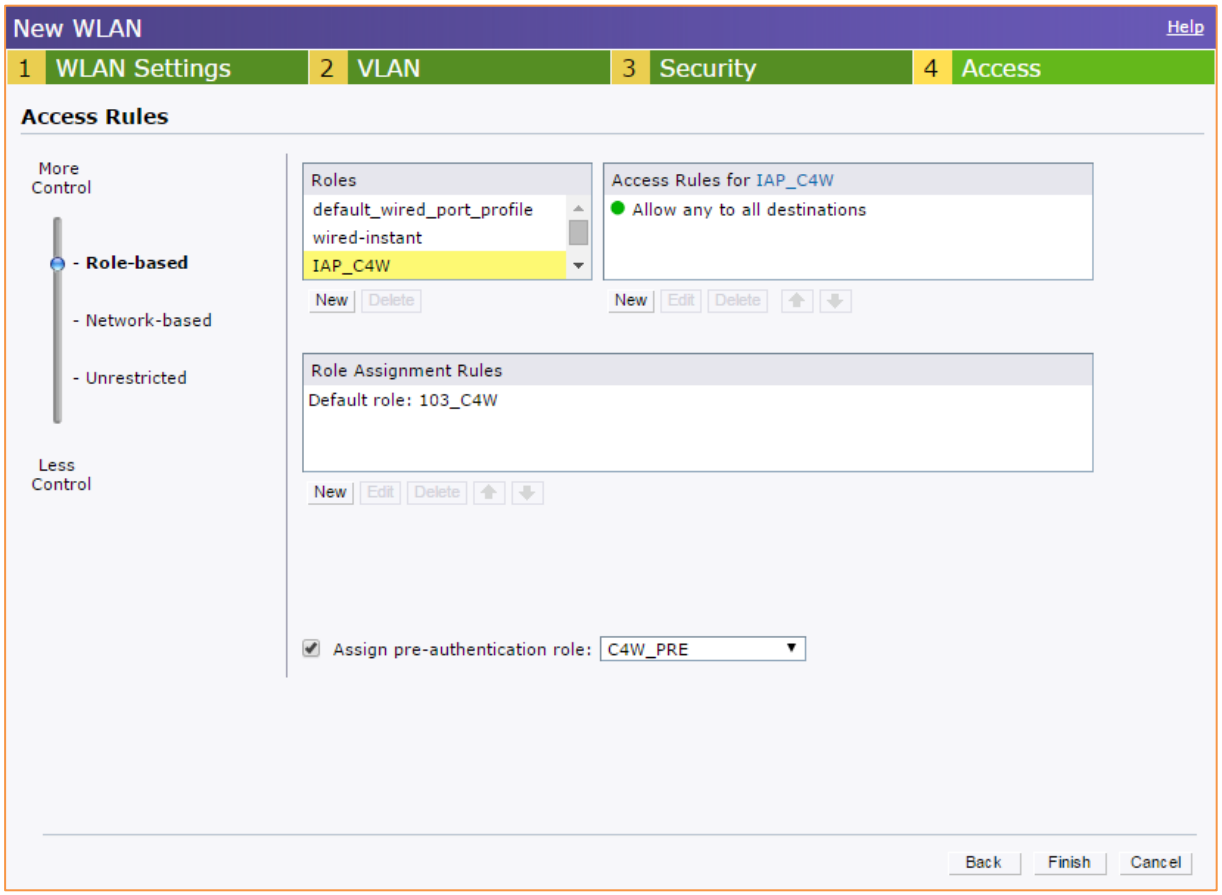
In de huidige firmware is het niet mogelijk https pagina's op te nemen in de walled garden. Omdat het IAP als proxy fungeert, gebruikt het zijn eigen certificaat voor alle https pagina's. Het gevolg hiervan is dat uw browser een certificaatfout geeft; de URL van de opgeroepen pagina wijkt immers af van de URL van het certificaat.

Om toch gebruik te kunnen maken van extra authenticatie opties op de Splash Portal van Cloud4Wi zoals Facebook, Twitter en Google+ kunt u gebruik maken van een access list. Access lists werken binnen het IAP op basis van rollen die aan de gebruikers toegewezen worden. In iedere rol staat beschreven wat de gebruiker wel en niet mag.
Tijdens de installatie wordt ten eerste aangegeven dat de toegang "role-based" is. Vervolgens worden er twee rollen aangemaakt, één rol voor en één rol na authenticatie. In de pre authentication role wordt toegang via https aan de gewenste authenticatie pagina's toegestaan en overige toegang geweigerd. Hoe dit precies in zijn werk gaat staat beschreven in de paragraaf "role-based access".

2.4 Role Based access

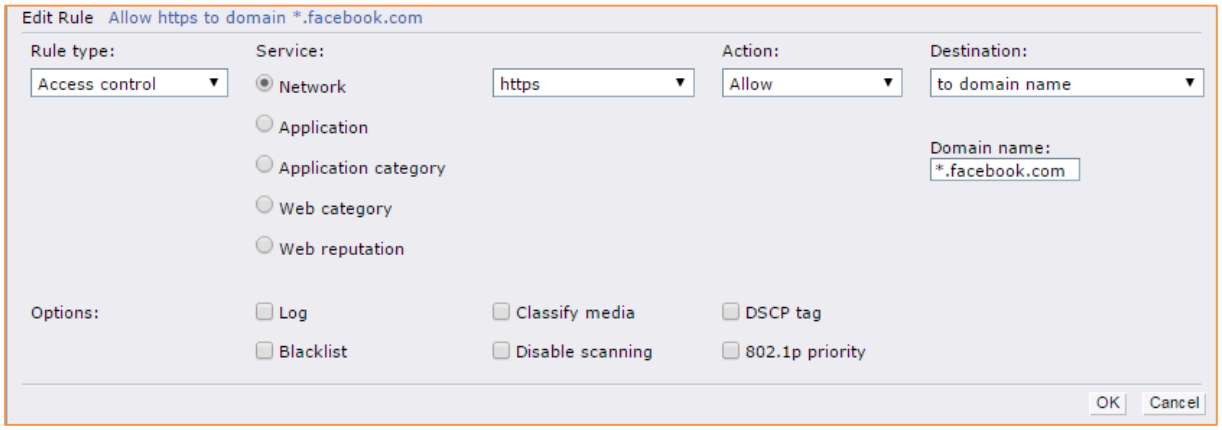
Zoals in de vorige paragraaf beschreven werkt de walled garden **"whitelist"** niet in combinatie met https pagina's. Om toch van deze functionaliteiten gebruik te maken moet de netwerk toegang **"Role-Based"** worden.

1. Kies hiervoor in het tabblad **"Access"** voor **"Role-based".**
2. Maak nu onder **"Roles"** 2 nieuwe rollen aan:
3. De rol die staat geselecteerd onder **"Roles"** is de rol die wordt toegewezen nadat de authenticatie succesvol is. Hier kunt u er voor kiezen om al het verkeer toe te staan.



Figuur 13: Access Rules

4. Onderaan wijst u een **"pre-authentication rol"** toe. Deze rol wordt aan de gebruiker toegewezen voordat authenticatie succesvol is. Hierin moeten een aantal dingen worden toegevoegd. Dit om ervoor te zorgen dat er geen toegang is tot het internet maar wel toegang tot de pagina's die nodig zijn om in te loggen, zoals bijvoorbeeld Facebook, Twitter of Google+.



Figuur 14: Edit rule

a. Allow **"http"** to **"172.31.98.1"** (gateway van de default DHCP-scope van gasten netwerk),
b. Allow **"TCP"** on port **"4343"** to **"172.31.98.1"** (gateway van de default DHCP-scope van gasten netwerk),
c. Allow **"DHCP"** to **"all",**
d. Allow **"DNS"** to **"all",**
e. Allow **"https"** to **"*.facebook.com",**
f. Voor bovenstaande regel kunt u alle onderstaande domeinen invullen, afhankelijk van de authenticatie optie die u wilt activeren.

Authenticatie Optie	Domeinen
Facebook	*.facebook.* *.fbcdn.* *.akamaihd.*
Twitter	*.twitter.* *.twimg.*
Google +	*.google.* *.googleapis.* *.gstatic.*
LinkedIn	*.linkedin.* *.licdn.*
VKontakte	*.vk.*
PayPal	*.paypal.* *.paypalobjects.*