

EXTERNE AUTHENTICATIE RUCKUS ZD WEBINTERFACE

Technote

Versie: 1.0
Auteur: Thomas Snijder
Datum: 28-04-2014

Inhoud

1	Inleiding	2
2	Configuratie	3
2.1	AAA SERVER.....	3
2.2	ROLLEN.....	4
2.3	WEBINTERFACE AUTHENTICATIE.....	5

1 Inleiding

In dit document wordt beschreven hoe u de ZoneDirector kunt configureren zodat deze beheeromgeving authenticatie uitvoert bij een externe authenticatieserver. Door deze gegevens te authenticeren bij een externe authenticatie server kunt u gemakkelijk rolebased toegang bieden. Dit kunt u doen door verschillende rollen te definiëren in de ZoneDirector en te kijken naar de groep waar de betreffende gebruiker bij hoort. Op deze manier kunt u de betreffende gebruiker volledige rechten geven in de ZoneDirector, of bijvoorbeeld alleen "kijk"-rechten op basis van de gedefinieerde rol.

Dit document gaat alleen in op de configuratie van de ZoneDirector en gaat niet in op het opzetten van een authenticatie server zoals een LDAP, Radius of Active Directory. Voor het opzetten van een Radius-server kunt u de volgende technote gebruiken:

[Ruckus FreeRadius Technote](#)

De instructies die in dit document gegeven worden gaan uit van een Engelstalige webinterface van de ZoneDirector. 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 firmware versie 9.7.0.0.220. Mocht u een lagere firmware hebben dan heeft u kans dat sommige functionaliteiten nog niet aanwezig zijn. Mocht u een hogere firmware versie hebben dan zullen de stappen nagenoeg hetzelfde zijn.

1.1 Doelstelling

De doelstelling van dit document is om de gebruiker bekend te maken met de configuratie mogelijkheden die het opzetten van externe authenticatie voor de beheerinterface van de ZoneDirector mogelijk maakt. Daarbij uitgaande van LDAP, Radius of Active Directory. Hiermee kan gecentraliseerde, rolebased toegang worden gerealiseerd.

1.2 Beoogd publiek

Dit document is geschreven voor technisch personeel / installateurs die de ZoneDirector webinterface authenticatie dienen te koppelen met reeds aanwezige authenticatie server omgevingen.

1.3 Voorkennis/Benodigdheden

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

- Authenticatieservers
- Ruckus GUI gebruik

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

- Ruckus ZoneDirector
- Internet Browser
- Authenticatieserver (deze wordt in dit document niet verder behandeld)

2 Configuratie

In de onderstaande hoofdstukken worden de stappen uitgelegd die doorlopen moeten worden voor het opzetten van externe authenticatie voor de webinterface.

2.1 AAA Server

De eerste stap voor het opzetten van de externe authenticatie is het configureren van een AAA server in de ZoneDirector. Uiteindelijk kunnen we deze authenticatie server koppelen aan de ZoneDirector zodat deze de inloggegevens kan valideren.

Voor het aanmaken van een authenticatieserver navigeert u naar **Configure -> AAA Servers**. Op deze pagina vindt u twee categorieën:

- Authentication/Accounting Servers
- Test Authentication Settings

Om een nieuwe authenticatie server aan te maken klikt u in de categorie **Authentication/Accounting Servers** op **Create New**.

In het veld **Name** geeft u de naam op voor de betreffende authenticatieserver.

Bij **Type** selecteert u het type authenticatie server.

In het veld **IP Address** geeft u het IP-adres op van de betreffende authenticatie server.

Daarna moet u eventueel nog poort-gegevens, wachtwoorden of domeinnamen opgeven. Doordat dit verschilt per authenticatie server gaan wij hier niet verder op in.

Na het toevoegen van de AAA server kunt u in de categorie **Test Authentication Settings** controleren of de ZoneDirector de authenticatie server kan bereiken. Ook kunt met deze optie controleren welke groeps-attributen u exact terug krijgt als u een gebruiker authentiseert.

2.2 Rollen

De AAA server is nu aangemaakt. Nu kunnen de rollen aangemaakt worden die definiëren wat de gebruikers wel en niet mogen als zij tot de betreffende rol horen. Voor het aanmaken van gebruikersrollen navigeert u naar **Configure -> Roles**.

Op deze pagina kunt u verschillende rollen aanmaken met verschillende rechten. Om een nieuwe rol aan te maken klikt u op **Create New**. Een nieuw venster wordt nu geopend.

In het veld **Name** geeft u de naam op voor de betreffende rol.

In het veld **Description** kunt u een omschrijving opgeven van de betreffende rol.

In het veld **Group Attributes** kunt u groeps-attributen opgeven die een Active Directory, LDAP of een Radius-server naar de ZoneDirector stuurt zodra een gebruiker geauthentiseerd is. Op basis van deze groeps-attributen bepaald de ZoneDirector bij welke "Role" de gebruiker hoort. Het is dus belangrijk dat het ingevoerde groeps-attributen exact overeenkomen met de attributen die de ZoneDirector ontvangt vanaf de authenticatie server.

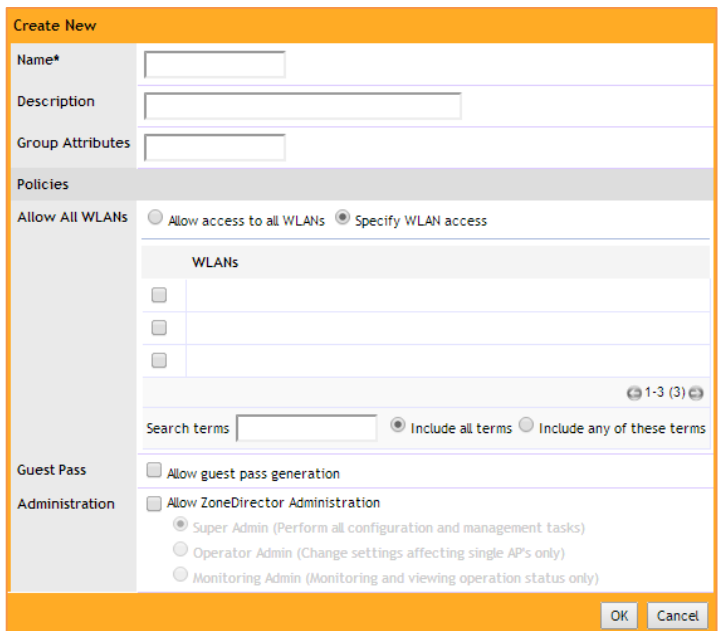
In de kolom **Policies** kunt u aangeven welke rechten de gebruikers hebben die tot deze rol behoren. Zo kunt u de gebruikers toegang geven tot alle WLANs door de optie **Allow access to all WLANs** aan te zetten. Als u wilt specificeren tot welke WLANs de gebruikers toegang mogen hebben, dan kunt u de optie **Specify WLAN access** aanzetten.

Als u voor de optie **Specify WLAN access** heeft gekozen, dan kunt u aangeven tot welke WLANs de gebruikers toegang hebben die bij deze rol horen.

Naast het specificeren tot welke WLANs de gebruikers toegang mogen hebben, kunt u ook aangeven of de gebruikers die behoren tot deze rol het recht hebben om gastcodes aan te maken. U kunt de gebruikers dit recht geven door de optie **Allow guest pass generation** aan te zetten.

Daarnaast kunt u specificeren of de gebruikers die behoren tot deze rol toegang mogen hebben tot de webinterface van de ZoneDirector. Om dit te activeren vinkt u de optie **Allow ZoneDirector Administration** aan. Daarna kunt u aangegeven welke rechten de betreffende gebruikers hebben in de webtinterface. U heeft hierbij de keuze uit:

- Super Admin
- Operator
- Monitoring



Figuur 1: Create New Role

2.3 Webinterface Authenticatie

Na het opzetten van de AAA server en het aanmaken van de rollen kunnen we nu de authenticatie voor de webinterface van de ZoneDirector aanpassen. Voor het aanpassen van de authenticatie navigeert u naar **Administer -> Preferences**.

Op deze pagina vindt u drie categorieën:

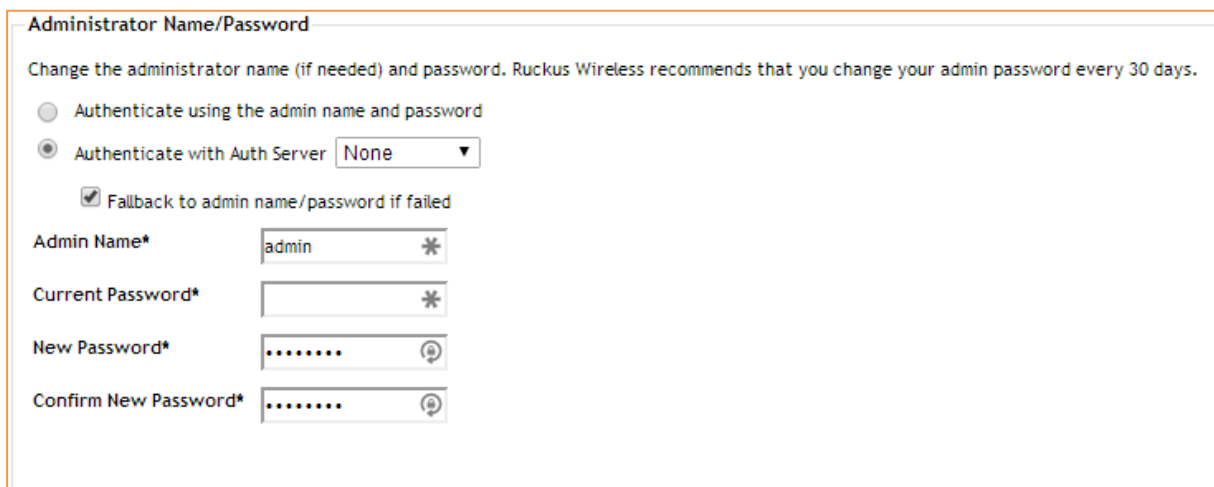
- Language
- Administrator Name/Password
- Administrator Session Timeout

Om de authenticatie instellingen voor de webinterface aan te passen gaat u te werk in de categorie Administrator Name/Password.

In deze categorie selecteert u de optie **Authenticate with Auth Server**. Daarna kunt u selecteren tegen welke server de ZoneDirector zijn inlog-verzoeken moet valideren. Hier selecteert u dus de eerder aangemaakte AAA server.

Let op:

Als u deze instellingen heeft gedaan is het aan te raden om de optie **Fallback to admin name/password if failed** aan te vinken. Door dit aan te zetten heeft u altijd de mogelijkheid om met het admin account in te loggen op de ZoneDirector, ook als uw authenticatie server offline is.



The screenshot shows the 'Administrator Name/Password' configuration page. At the top, it says 'Change the administrator name (if needed) and password. Ruckus Wireless recommends that you change your admin password every 30 days.' There are two radio button options: 'Authenticate using the admin name and password' (unselected) and 'Authenticate with Auth Server' (selected). The 'Authenticate with Auth Server' option has a dropdown menu currently set to 'None'. Below these options is a checked checkbox for 'Fallback to admin name/password if failed'. At the bottom, there are four input fields: 'Admin Name*' with the value 'admin', 'Current Password*', 'New Password*' (masked with dots), and 'Confirm New Password*' (masked with dots). Each input field has a small icon to its right, likely for password strength or visibility toggles.

Figuur 2: Change Webinterface Authentication