

RUCKUS DPSK + ZERO-IT

Technote

Versie: 1.1
Auteur: Thomas Snijder
Datum: 17-02-2014

Inhoud

- 1 Inleiding 2
- 2 Configuratie 3
 - 2.1 CAPTIVE PORTAL 3**
 - 2.1.1 ENABLE GUEST ACCESS 3
 - 2.2 WLAN 4**
 - 2.3 USERS & ROLES 7**
 - 2.3.1 ROLES 7
 - 2.3.2 USERS 8
- 3 Inloggen 9

1 Inleiding

In dit document wordt beschreven hoe u Dynamic-PSK WLAN kunt configureren op de ZoneDirector van Ruckus Wireless. Dynamic-PSK zorgt ervoor dat elke medewerker een eigen PSK (Pre Shared Key) heeft om verbinding te maken met het Wi-Fi netwerk. Door Dynamic-PSK te gebruiken wordt uw Wi-Fi netwerk vele malen veiliger omdat elke medewerker zijn eigen code heeft. De codes kunt u maximaal 62 karakter lang maken, dit maakt de codes minder gevoelig voor brute force attacks. Simpelweg omdat er teveel mogelijkheden zijn en het veel tijd kost om alle mogelijkheden te proberen.

Om deze Dynamic-PSK codes gemakkelijk aan te bieden bij de medewerkers, heeft Ruckus de functie Zero-IT geïmplementeerd. Zero-IT geeft de medewerker de mogelijkheid om een Wi-Fi profiel te downloaden van de ZoneDirector nadat de medewerker geauthenticeerd is. Dit Wi-Fi profiel dient geïnstalleerd te worden op de telefoon, tablet of laptop. Het profiel zal er dan voor zorgen dat de lange Dynamic-PSK code geïnstalleerd wordt op het betreffende device. Tevens wordt deze Dynamic-PSK code gekoppeld aan het betreffende device op basis van het mac-adres, het is dus niet mogelijk om een uitgegeven code over te zetten naar een ander device.

Naast het feit dat de Dynamic-PSK codes aan een mac-adres gekoppeld worden, kan de beheerder van de ZoneDirector ook aangeven hoeveel Dynamic-PSK codes een medewerker mag aanvragen.

Het registreren van hardware voor een Dynamic-PSK WLAN wordt gedaan via een gastennetwerk. Dit is nodig omdat een medewerker eerst verbinding moet maken met de ZoneDirector om zo het betreffende Wi-Fi profiel op te halen.

Voor het opzetten van een Dynamic-PSK WLAN is basiskennis van de ZoneDirector vereist. Zoals het verschil weten tussen de verschillende tabs en waar de verschillende configuratie-opties zich bevinden. Daarnaast is het aan te raden om basiskennis van netwerken te hebben voor het inrichten van het Dynamic-PSK WLAN, dit is alleen van toepassing als er bijvoorbeeld een apart VLAN toegekent moet worden aan het Dynamic-PSK WLAN.

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 9.6.1.0.15. 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.

2 Configuratie

In de onderstaande hoofdstukken worden de stappen uitgelegd die doorlopen moeten worden voor het opzetten van een Dynamic-PSK WLAN.

2.1 Captive portal

De eerste stap voor het opzetten van een Dynamic-PSK WLAN is het configureren van de captive portal voor het gastennetwerk. Het gebruik van de ingebouwde captive portal van Ruckus maakt het hele proces een stuk makkelijker. Wanneer een nieuwe gebruiker gebruik wil maken van het gastennetwerk zal de captive portal zichtbaar worden op het device. In de portal heeft de gebruiker de mogelijkheid een device te registreren.

Uw gasten kunnen ook nog steeds met dit netwerk verbinden, omdat er op de captive portal ook een optie staat om gasten toegang te krijgen via een voucher code.

De instellingen voor de captive portal kunt u vinden onder **Configure -> Guest Access**. Op deze pagina vindt u verschillende categorieën:

- Enable Guest Access
- Guest Pass Generation
- Restricted Subnet Access
- Web Portal Logo
- Guest Access Customization
- Guest Pass Printout Customization

Om een captive portal op te zetten met de Zero-IT functionaliteit moet één categorie worden aangepast. Hieronder wordt uitgelegd welke instellingen u moet aanpassen.

2.1.1 Enable Guest Access

In deze categorie kunt u aangeven wat voor functies de captive portal moet aanbieden. Wij zullen hieronder een toelichting geven over de verschillende opties die in deze categorie aangepast moeten worden:

Onboarding Portal: deze optie biedt u de mogelijkheid om devices te registreren voor een Dynamic PSK WLAN. Het is belangrijk dat u deze optie aanzet. Hierdoor kunnen uw medewerkers gemakkelijk een Dynamic-PSK WLAN profiel opvragen voor hun device.

Authentication: deze optie biedt u de mogelijkheid om te specificeren of uw gasten doormiddel van een code toegang te geven tot het internet. Het is belangrijk dat u deze optie op **Use guest pass authentication** zet. Hierdoor krijgen uw gebruikers de keuze tussen gasten toegang, of het registreren van een device.

De bovenstaande instellingen zijn nodig voor het gebruik van Zero-IT. Alle andere instellingen op deze pagina zijn van toepassing op het gastengedeelte van de captive portal. De inrichting van een gastennetwerk en de uitleg van de overige functies wordt besproken in de technote "[Alcadis – Ruckus Guest Access Technote](#)".

2.2 WLAN

In het bovenstaande hoofdstuk hebben wij uitgelegd welke instellingen u moet aanpassen om de Zero-IT optie toe te voegen aan de captive portal. In dit hoofdstuk beschrijven wij hoe u een WLAN kunt aanmaken dat gebruik maakt van de captive portal met Zero-IT functionaliteit. Daarnaast beschrijven wij hoe u een Dynamic-PSK WLAN aan kunt maken. Om een WLAN aan te maken navigeert u naar **Configure -> WLANs**.

Op deze pagina klikt u in de categorie WLANs op **Create New**. Er zal een scherm openklappen voor het aanmaken van een nieuw WLAN.

In de velden **Name** en **ESSID** geeft u de naam op van uw gastennetwerk. De naam die u invult in het veld **ESSID** zal de naam zijn die zichtbaar is voor uw gebruikers.

In het veld **Description** kunt u een omschrijving invullen van het betreffende WLAN. Het invullen van een omschrijving is niet verplicht.

Bij **Type** selecteert u **Guest Access**. Door Guest Access te selecteren worden de instellingen die u eerder heeft gedaan bij **Configure -> Guest Access** geactiveerd.

De basisinstellingen voor het gastennetwerk zijn nu gedaan, eventueel kunt u nog onder **Advanced Options** extra instellingen doen voor het gasten netwerk. Onder advanced options kunt u bijvoorbeeld een bandbreedte beperking activeren. Ook heeft u de mogelijkheid om onder de advanced options het gastennetwerk in een apart VLAN te laten opereren. Door dit te doen kunt u ervoor zorgen dat uw gastennetwerk via een aparte internetverbinding naar buiten gaat.

De overige categorieën die zichtbaar zijn op de WLANs pagina zijn niet van toepassing op het aanmaken van een gastennetwerk. De functies van deze categorieën worden daarom niet beschreven in dit document.

The screenshot shows a web-based configuration form for creating a new WLAN. The form is titled "Create New" and is organized into several sections:

- General Options:** Contains two input fields: "Name/ESSID*" and "Description".
- WLAN Usages:** Contains a "Type" section with four radio button options: "Standard Usage (For most regular wireless network usages.)", "Guest Access (guest access policies and access control will be applied.)", "Hotspot Service (WISPr)", and "Hotspot 2.0".
- Authentication Options:** Contains a "Method" section with four radio button options: "Open", "802.1x EAP", "MAC Address", and "802.1x EAP + MAC Address".
- Encryption Options:** Contains a "Method" section with six radio button options: "WPA", "WPA2", "WPA-Mixed", "WEP-64 (40 bit)", "WEP-128 (104 bit)", and "None".
- Options:** Contains two sections: "Wireless Client Isolation" with three radio button options ("None", "Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.)", "Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.)") and "Priority" with two radio button options ("High", "Low").
- Advanced Options:** A link to expand the form.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Figuur 1: Create New WLAN

Het gastennetwerk is nu aangemaakt, maar er moet nog een Dynamic-PSK netwerk aangemaakt worden. Om dit te doen navigeert u naar **Configure -> WLANs**.

Op deze pagina klikt u in de categorie WLANs op **Create New**. Er zal een scherm openklappen voor het aanmaken van een nieuw WLAN.

In de velden **Name** en **ESSID** geeft u de naam op van uw Dynamic-PSK WLAN. De naam die u invult in het veld **ESSID** zal de naam zijn die zichtbaar is voor uw gebruikers.

In het veld **Description** kunt u een omschrijving invullen van het betreffende WLAN. Het invullen van een omschrijving is niet verplicht.

Bij **Type** selecteert u **Standard Usage**.

Bij **Authentication Method** selecteert u **Open**.

Bij **Encryption Method** selecteert u **WPA2**.

Bij **Algorithm** selecteert u **AES**.

Bij passphrase geeft u een wachtwoord op voor het Dynamic-PSK WLAN. Dit wachtwoord heeft u later niet meer nodig, dus u kunt hier blind een wachtwoord intypen.

Na deze instellingen zet u de optie **Enable Zero-IT Activation** aan, deze optie vindt u onder **Options**.

Na het activeren van **Enable Zero-IT Activation**, krijgt u de optie **Enable Dynamic-PSK** te zien. Ook deze vinkt u aan, daarnaast kunt u aangeven hoelang de Dynamic-PSK sleutel moet zijn. Wij adviseren u om deze waarde op 62 te laten staan.

Na het activeren van **Enable Dynamic-PSK**, krijgt u de optie **Limit D-PSK generation per user to ... devices** te zien. Het is niet verplicht om deze optie aan te zetten, maar hiermee kunt u het aantal Dynamic-PSK verzoeken limiteren per medewerker.

The screenshot shows the 'Create New' configuration window for a WLAN. It includes the following sections and settings:

- General Options:** Name/ESSID* (input field), Description (input field).
- WLAN Usages:** Type: Standard Usage (For most regular wireless network usages.), Guest Access (Guest access policies and access control will be applied.), Hotspot Service (WISPr), Hotspot 2.0.
- Authentication Options:** Method: Open, 802.1x EAP, MAC Address, 802.1x EAP + MAC Address.
- Encryption Options:** Method: WPA, WPA2, WPA-Mixed, WEP-64 (40 bit), WEP-128 (104 bit), None. Algorithm: TKIP, AES, Auto. Passphrase* (input field).
- Options:** Web Authentication: Enable captive portal/Web authentication (Users will be redirected to a Web portal for authentication before they can access the WLAN.). Authentication Server: Local Database. Wireless Client Isolation: None, Local (Wireless clients associated with the same AP will be unable to communicate with one another locally.), Full (Wireless clients will be unable to communicate with each other or access any of the restricted subnets.). Zero-IT Activation™: Enable Zero-IT Activation (WLAN users are provided with wireless configuration installer after they log in.). Dynamic PSK™: Enable Dynamic PSK with 62 characters passphrase. Limit D-PSK: Limit D-PSK generation per user to 3 devices. Priority: High, Low. [Advanced Options](#) link.

Figuur 2: Create New WLAN

De basisinstellingen voor het Dynamic-PSK WLAN zijn nu gedaan, eventueel kunt u nog onder Advanced Options extra instellingen doen voor het Dynamic-PSK WLAN. Zoals het toewijzen van een VLAN.

Onder de categorie **Zero-IT Activation** kunt u nog aanvullende instellingen doen met betrekking tot de authenticatie van de medewerkers.

Authentication Server: Via deze optie kunt u specificeren tegen welke database uw medewerkers geauthenticeerd moeten worden. Voor een standaard Dynamic-PSK WLAN kunt u deze optie op **Local Database** laten staan. Heeft u binnen het netwerk een Active Directory, LDAP of een Radius server draaien, dan kunt u deze toevoegen onder **Configure -> AAA Servers**. Na het toevoegen van een AAA Server kunt u deze server selecteren als **Authentication Server**. Uw medewerkers worden dan geauthenticeerd tegen deze server om toegang te krijgen tot het Zero-IT profiel.

Het opzetten en toevoegen van een Active Directory, LDAP of Radius server wordt niet behandeld in deze technote.

Onder de categorie **Dynamic PSK** kunt u nog opgeven hoelang een Dynamic-PSK sleutel geldig is na activatie.

2.3 Users & Roles

2.3.1 Roles

Het Dynamic-PSK WLAN is nu volledig geconfigureerd en kan gebruikt worden door de medewerkers. Het laatste wat nu nog gedaan moet worden is het aanmaken van gebruikers die rechten hebben op het betreffende Dynamic-PSK WLAN. Om dit realiseren moeten er eerste gebruikersrollen worden aangemaakt. 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 groepsattributen opgeven die een Active Directory, LDAP of een Radius server naar de ZoneDirector kunnen sturen. Als de ZoneDirector een request ontvangt van deze server, dan gaat de ZoneDirector kijken op basis van de groepsattributen welke rol het beste bij de betreffende gebruiker past. Zowel de omschrijving als de groepsattributen zijn geen verplichte velden.

Het gebruik van groepsattributen is alleen van toepassing als er gebruik gemaakt wordt van een **AAA Server** voor het authenticeren van gebruikers.

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.

Als u ook wilt dat de betreffende gebruikers administrator rechten op de ZoneDirector hebben, dan kunt u de optie **Allow ZoneDirector Administration** aanzetten.

Wanneer u een rol aanmaakt die de gebruiker het recht geeft om gastcodes aan te maken, dan moet u ervoor zorgen dat het betreffende gastennetwerk aangevinkt is onder **Policies**, daarnaast is het belangrijk dat de optie **Allow guest pass generation** aanstaat.

The screenshot shows the 'Create New' dialog box for creating a role. It includes fields for Name, Description, and Group Attributes. Under Policies, the 'Specify WLAN access' option is selected. Below this is a table of WLANs with checkboxes. There is also a search bar and radio buttons for search terms. Under Guest Pass, the 'Allow guest pass generation' checkbox is present. Under Administration, the 'Allow ZoneDirector Administration' checkbox is present, along with radio buttons for Super Admin, Operator Admin, and Monitoring Admin. The dialog has OK and Cancel buttons at the bottom right.

Figuur 3: Create New Role

2.3.2 Users

Nu de rol voor het Dynamic-PSK WLAN is aangemaakt moeten er nog gebruikers worden aangemaakt die aan deze rol zijn gekoppeld. Voor het aanmaken van gebruikers navigeert u naar **Configure -> Users**.

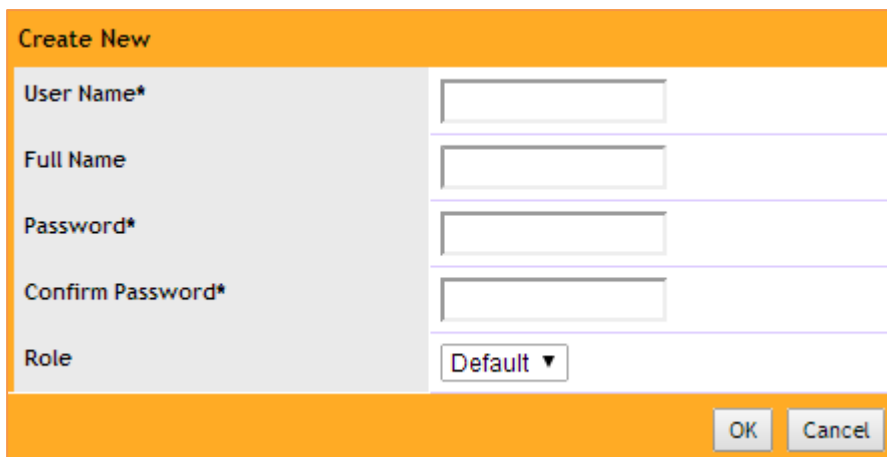
Op deze pagina kunt u gebruikers aanmaken, voor het aanmaken van een nieuwe gebruiker klikt u op **Create New**. Een nieuw venster wordt nu geopend.

In het veld **Username** geeft u de gebruikersnaam voor de betreffende gebruiker op.

In het veld **Full Name** kunt u de volledige naam opgeven van de gebruiker. Het invullen van dit veld is niet verplicht.

In het veld **Password** en **Confirm Password** geeft u het gewenste wachtwoord op voor de gebruiker.

In het pulldown menu genaamd **Role** selecteert u de eerder aangemaakte rol met de rechten voor het betreffende Dynamic-PSK WLAN.



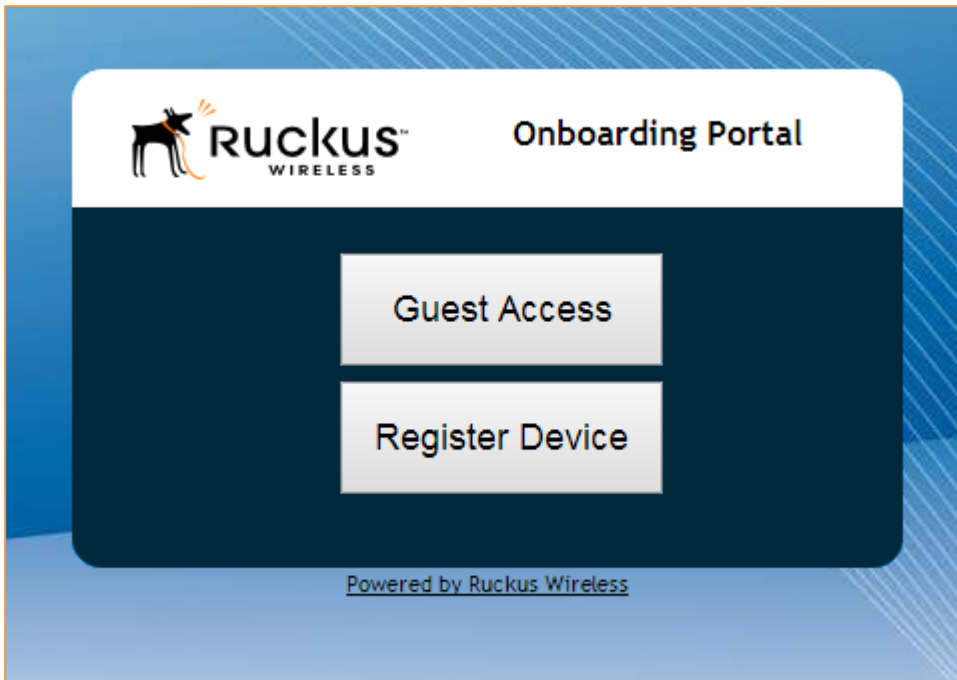
The image shows a 'Create New' dialog box with an orange header and footer. The main content area is white with a light gray sidebar on the left. The sidebar contains the following labels: 'User Name*', 'Full Name', 'Password*', 'Confirm Password*', and 'Role'. Each label is followed by a corresponding input field: a text box for 'User Name', a text box for 'Full Name', a text box for 'Password', a text box for 'Confirm Password', and a dropdown menu for 'Role' currently showing 'Default'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Figuur 4: Create New User

3 Inloggen

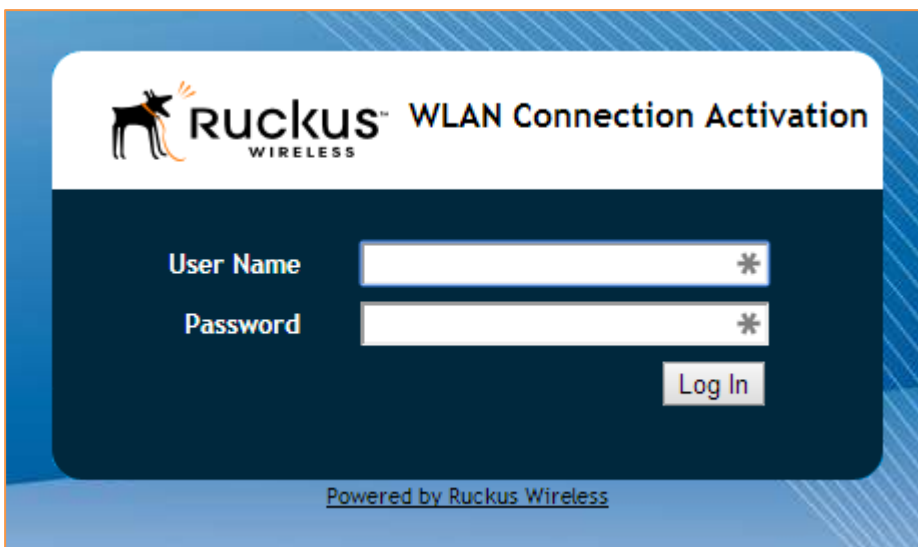
In het onderstaande hoofdstuk wordt uitgelegd hoe u kunt inloggen op de ZoneDirector en het betreffende Dynamic-PSK WLAN profiel kunt downloaden.

Om een Dynamic-PSK WLAN profiel te downloaden maakt u verbinding met het aangemaakte gastennetwerk. Na het verbinden met het gastennetwerk opent u de internet browser. Als u nu naar een willekeurige website gaat wordt u geredirect naar de captive portal van de ZoneDirector, waarbij u twee keuzes krijgt. U kiest hiervoor **Register Device**.



Figuur 5: Onboarding Portal

Als u op **Register Device** heeft geklikt krijgt u een inlogscherm te zien. Hier vult u de gegevens in van een eerder aangemaakte gebruiker.



Figuur 6: Login

Als de gegevens van deze gebruiker geaccepteerd worden, krijgt u een nieuwe pagina te zien.

RUCKUS™
WIRELESS

Corporate WLAN Configuration

To set up your wireless network connection, follow these steps:

- If the WLAN Connector download does not start in five seconds, please [click here](#).
- Save prov.exe to your desktop. Once completed, go to your desktop, double-click the prov.exe icon.
- After your network connection is activated, the wireless icon (in the system tray) will change. Your computer will be automatically reconnected to the secured corporate network.

prov.exe

Disconnected Connecting Connected

- If you encounter any problem or would like to manually set up your wireless access, [click here](#)

Powered by Ruckus Wireless

Figuur 7: Zero-IT Profiel

Zodra deze pagina geladen is krijgt u een download aangeboden, die het profiel bevat voor het Dynamic-PSK WLAN. Nadat u dit bestand heeft gedownload kunt u het programma uitvoeren op het betreffende device. Het programma zal nu een WLAN profiel installeren. Nadat het programma het WLAN profiel heeft geïnstalleerd kunt u verbinding maken met het Dynamic-PSK WLAN.

Mocht uw device niet worden herkend worden het Ruckus Zero-IT proces, dan heeft u nog de optie om handmatig de unieke Dynamic-PSK code te kopiëren. Deze code kunt u dan plakken in het wachtwoordveld als u verbinding wilt maken met het Dynamic-PSK netwerk.