

# SpeedTouch 580

## Standaard WPA beveiliging ingesteld

### 1 Beveiliging

#### 1.1 Beveiliging instellen of wijzigen met SpeedTouch 580 (ADSL)

- 1 Open Internet Explorer (of een andere browser) en vul op de adresbalk het adres **http://10.0.0.138** in en druk op Enter. **Typ geen www!**
- 2 Als er een inlogscherf verschijnt, vult u de standaard gebruikersnaam en standaard geen wachtwoord in, of vul het door u aangemaakte wachtwoord in.
- 3 Klik in de linker kolom op **Basic**.
- 4 Klik in de linker kolom op **Wireless**.
- 5 Klik in het kader op het tabblad **Security**.

#### 1.2 Voor WPA en WPA2 beveiliging

- 1 Klik daarna op het driehoekje voor de tekst **Security Level 2- WPA-PSK (WPA Personal)**.
- 2 Selecteer achter **Encryption**: de gewenste versleuteling **TKIP** of **AES** in. AES is nieuwer en daardoor veiliger, maar oudere draadloze apparaten kunnen hier niet altijd mee overweg.
- 3 Vul achter **WPA passphrase**: een door u verzonden sleutel in.
- 4 Klik op **Apply**.
- 5 Klik linksboven het menu op **Save All**.

#### 1.3 Voor WEP-beveiliging

- 1 Klik daarna op het driehoekje voor de tekst **Security Level 1- WEP**.
- 2 Selecteer achter **Type**: het gewenste type WEP-sleutel. De Alphanumeric methode wordt niet door alle draadloze apparaten ondersteund.
- 3 Vul achter **Encryption Key**: de juiste sleutel in (10 karakters bij 64 bit en 26 karakters bij 128 bit).
- 4 Klik op **Apply**.
- 5 Klik linksboven het menu op **Save All**.

### 2 Beveiliging van het draadloze netwerk

Als de SpeedTouch 580 geconfigureerd is met de bijgeleverde CD-rom Installatie Wireless-modem Alcatel ST580 (versie 4.2.1) is het modem beveiligd. De draadloze informatie wordt versleuteld met een 64 bit WPA sleutel, bestaande uit cijfers en letters. Met deze beveiliging is het vrijwel onmogelijk dat derden uw draadloos verzonden informatie kunnen ontcijferen en dat iemand zich ongewenst draadloos toegang kan verschaffen tot uw modem en netwerk.

### 3 Het modem nog beter beveiligen

De modem kent 3 beveiligingsmogelijkheden. Hieronder wordt aangegeven hoe u het modem nog beter kunt beveiligen.

#### 3.1 Netwerknnaam

Het modem zendt zijn netwerknnaam (SSID) uit. Hierdoor is het draadloze netwerk zichtbaar voor iedereen die zich met een WiFi apparaat binnen het bereik van het modem bevindt. U kunt dit uitschakelen;

Typ in uw Internet Explorer (of een andere browser) **http://10.0.0.138** en u komt in het menu van het modem. **Typ geen www!** Klik op **Wireless** in de linker tabel. Er verschijnt een scherm met drie tabbladen. In het tabblad **Access Point Settings** plaatst u een vinkje achter: **Only stations with correct Network Name (SSID) can connect**. Klik op **Apply** en hierna op **Save All**. Uw draadloze netwerk is nu niet meer zichtbaar voor anderen.

### 3.2 WEP/WPA beveiliging

U kunt de standaard geactiveerde WEP/WPA-sleutel van 10 karakters veranderen. Bij het gebruik van WPA is het mogelijk om een wachtwoord in te geven die uit minimaal 8 en maximaal 63 karakters bestaat. Het veiligst is het ingeven van 63 karakters. Als u de sleutel in het modem vervangt moet dit ook gebeuren op alle andere aangesloten computers.

Typ in uw Internet Explorer (of een andere browser) <http://10.0.0.138> en u komt in het menu van de modem. **Typ geen www!** Klik op **Wireless** in de linker tabel. Er verschijnt een scherm met drie tabbladen. In het tabblad **Security** klikt u op het driehoekje voor **Security Level 2**. In het veld WPA passphrase ziet u de standaard beveiligingscode van 10 karakters staan, verander deze in een zin van 63 karakters. Klik op **Apply**.

De draadloze verbinding van uw computer met het modem bent u nu kwijt. Om de verbinding te herstellen moet u de WEP-sleutel in uw computer aanpassen;

Klik op de snelkoppeling **SpeedTouch 110g Wireless PC Card Monitor** of **SpeedTouch 120g Wireless USB Monitor**. Klik op het tabblad **Security** en geef in het veld **Shared Secret Key (PSK)** de nieuwe sleutel in. Klik op de button **Apply Change**. Herstart de computer.

### 3.3 Access Control List (toegangslijst) en registratiebutton

Met behulp van de toegangslijst kunt u bepalen wie er verbonden zijn met het draadloze netwerk en hoe nieuwe gebruikers zich moeten aanmelden. Er zijn 3 instellingen mogelijk voor de toegangslijst. De veiligste optie is **New stations allowed (via registration)**. Als u deze optie activeert, kan een nieuwe gebruiker alleen verbonden worden met uw draadloze netwerk als de knop voorop uw modem 4 seconden ingedrukt wordt. Na het indrukken van de knop staat de toegangslijst 1 minuut open.

Typ in uw Internet Explorer (of een andere browser) <http://10.0.0.138> en u komt in de webinterface van het modem. **Typ geen www!** Klik op **Wireless** in de linker tabel, er verschijnt een scherm met drie tabbladen. Klik vervolgens op het tabblad **Security**, en **Access Control**. Hier kunt u de optie activeren die u wenst.

## 4 Het verschil tussen WEP, WPA en WPA2

WEP, WPA en WPA2 zijn versleutelingsmethodes om draadloos netwerkverkeer te beveiligen. Wanneer u een WEP-sleutel gebruikt, wordt de data met één en dezelfde sleutel versleuteld. Wat ontvangen wordt moet dan eerst worden ontcijferd met deze sleutel. Een WEP-sleutel is door computers met veel rekenkracht op lange termijn te kraken.

Bij WPA-encryptie wordt er met sleutels gewerkt die om de 4 seconden wisselen. Hierdoor hebt u een hoge mate van veiligheid aangezien er geen tijd is om de gebruikte sleutel te kraken. Dit gebeurt volledig automatisch. Om verbinding te maken met het netwerk, maakt u gebruik van een vast wachtwoord. Voor de sleutel kunnen alle cijfers en letters worden gebruikt, inclusief de meeste speciale karakters en spaties. Deze sleutel bevat meestal tussen de 8 en 63 karakters en moet exact hetzelfde aan beide zijden van de verbinding worden ingevuld. Deze sleutel is moeilijker te achterhalen vanwege de vele mogelijkheden. Tijdens de gehele duur van de verbinding zullen het draadloze modem en het draadloos aangesloten apparaat constant nieuwe sleutels met elkaar afspreken. Voor elk aangemeld draadloos apparaat zijn dit andere sleutels. Dit heeft wel als nadeel dat het bij het verlies van de draadloze verbinding soms vrij lang kan duren voor de draadloze verbinding wordt hersteld, beide kanten moeten hiervoor weer terug naar de vooraf ingestelde sleutel.

WPA2 is de opvolger van WPA en maakt gebruik van hetzelfde principe als WPA dat de sleutel regelmatig verandert. WPA2 maakt gebruik van een andere berekening en gebruik van een wisselend aantal bits voor deze sleutel.