EMINENT

HANDLEIDING

EM4450 - Draadloze Router

WWW.EMINENT-ONLINE.COM

EM4450 - Draadloze Router

Waarschuwingen en aandachtspunten

Als gevolg van Europese regelgeving kan een draadloos product in sommige Europese lidstaten onderwerp zijn van beperkingen. Ook kan het gebruik van dit product in sommige Europese lidstaten in het geheel verboden zijn. Het openen van het product en/of de producten kan leiden tot ernstige verwondingen! Laat een reparatie altijd uitvoeren door gekwalificeerd personeel van Eminent!

Inhoudsopgave

Eminent Advanced Manual voor netwerkinstellingen en uitgebreide informatie over thuisnetwerken vanaf pagina 17.

1.0 Garantievoorwaarden

De garantietermijn van vijf jaar geldt voor alle Eminent producten, tenzij anders aangegeven op het moment van aankoop. Bij aankoop van een tweedehands Eminent product resteert de garantieperiode gemeten vanaf het moment van de aankoop door de eerste eigenaar.
De Eminent garantieregeling is van toepassing op alle Eminent producten en onderdelen onlosmakelijk verbonden met het betreffende product. Voedingen, batterijen, accu's, antennes en alle andere producten niet geïntegreerd in of direct verbonden met het hoofdproduct of producten waarvan redelijkerwijs mag worden aangenomen dat deze een ander slijtagepatroon kennen dan het hoofdproduct vallen derhalve niet onder de Eminent garantieregeling. De garantie vervalt tevens bij onjuist of oneigenlijk gebruik, externe invloeden en/of bij opening van de behuizing van het betreffende product door partijen anders dan Eminent.

2.0 Introductie

Gefeliciteerd met de aankoop van dit hoogwaardige Eminent product! Dit product is door de technische experts van Eminent uitgebreid getest. Mocht dit product ondanks alle zorg problemen vertonen, dan kun je een beroep doen op de vijf jaar Eminent garantie. Bewaar deze handleiding samen met het bewijs van aankoop daarom zorgvuldig.

Registreer je aankoop nu op www.eminent-online.com en ontvang product updates!

3.0 Functies en kenmerken

3.1 Inhoud van de verpakking

Je hebt gekozen voor de EM4450. Controleer of alle onderdelen in het pakket aanwezig zijn, alvorens met de installatieprocedure te beginnen.

- EM4450, draadloze router.
- Lichtnetadapter.
- UTP netwerkkabel.
- CD-ROM met installatiewizard en handleidingen.
- Gebruikershandleiding.

3.2 Functies en kenmerken

De EM4450 is ideaal om in een handomdraai je eigen, beveiligde draadloze netwerk te creëren. De EM4450 is een draadloos basisstation om jouw hele huis te voorzien van een draadloos netwerk. De prestaties van deze router zijn van hoog niveau waardoor je een stabiel en soepel draadloos netwerk kunt opbouwen.

Geniet van je netwerk en laat de EM4450 het werk doen!

- Ingebouwd 54Mbps accesspoint voor het opbouwen van een draadloos netwerk.
- Ingebouwde router voor het probleemloos delen van een internetverbinding.
- Ingebouwde 4 poorts switch voor het opbouwen van een bedraad netwerk.
- Ingebouwde Firewall ter bescherming van uw gegevens.

4.0 De router aansluiten

1. Schakel je computer uit.
2. Sluit de EM4450 middels de meegeleverde lichtnetadapter aan op het stopcontact.
3. Sluit de meegeleverde UTP netwerkkabel aan op de 'WAN'-poort van de EM4450.
4. Sluit de andere kant van deze UTP netwerkkabel aan op de LAN-poort van je bestaande kabelmodem.
5. Sluit een UTP netwerkkabel aan op één van de vier 'LAN'-poorten van je EM4450.
6. Sluit de andere kant van deze UTP netwerkkabel aan op de netwerkadapter in je computer.

Tip: Voor je gaat beginnen met het installeren van de EM4450 moet je controleren of deze juist op het lichtnet is aangesloten. Dit controleer je door te verifiëren of het lampje gemarkeerd met het universele stand-by pictogram brandt. Controleer ook of je netwerkkabel goed op je EM4450 en PC is aangesloten. Om dit te controleren start je de computer op, en controleer je of het lampje brandt dat correspondeert met de 'LAN'-poort waarop je de netwerkkabel hebt aangesloten.

5.0 EM4450 installeren via de CD.

Je stelt de EM4450 in als draadloze router als je beschikt over een kabel of ADSL modem. De makkelijkste manier om de EM4450 te installeren is met behulp van de installatiewizard, zoals staat beschreven in onderstaand hoofdstuk. Indien je bij de installatie van de EM4450 geen gebruik wilt maken van de wizard op de meegeleverde cd-rom, kun je de router ook handmatig installeren. Zie hoofdstuk 5.2.

1. Schakel je computer in.
2. Plaats de cd-rom in de cd-rom speler.
3. De wizard wordt gestart.
4. Volg de stappen op het scherm totdat de installatie voltooid is. Je hebt nu een werkende internetverbinding.

Tip: Wanneer de installatie CD-ROM niet automatisch start, dan kun je het installatieprogramma ook handmatig opstarten. Dit doe je als volgt:

1. *Klik op de 'Start'.*
2. *Klik op 'Uitvoeren'.*
3. *Typ x:\wizard\wizard.exe (waarbij 'x' de schijfletter van je CD-ROM of dvd-station is).*
4. *Klik op 'OK'.*

6.0 De router handmatig installeren

We gaan nu de verschillende methodes bespreken die mogelijk zijn om je EM4450 in te stellen. Heb je een provider met een dergelijke instellingsmethode, dan hoef je alleen maar de stappen te volgen welke worden behandeld. Dan ben je snel en veilig online!

Voorbeelden van providers die gebruik maken van DHCP als verbindingsmethode zijn: @Home, Zeelandnet, Casema Wanadoo en UPC Chello.

6.1 Inloggen op de EM4450

Voor de handmatige installatie van de EM4450 is het van belang dat je internetbrowser en je netwerk goed zijn geconfigureerd. De instellingen staan automatisch goed, tenzij je in het verleden iets hebt veranderd.

Tip! Zie de 'Advanced Manual' op de cd-rom als je twijfelt of je internetbrowser en je netwerk goed zijn ingesteld.

Je maakt handmatig verbinding met de EM4450 door de onderstaande procedure te volgen.

1. Schakel je computer in.
2. Open je internetbrowser (Bijvoorbeeld Internet Explorer, Netscape of Firefox).
3. Typ ' http://192.168.1.1 ' in de adresbalk.
4. Druk op de entertoets of klik op 'Ga naar'.
5. Typ 'admin' bij gebruikersnaam.
6. Typ 'admin' bij wachtwoord.
7. Klik op 'OK'.
8. Het openingsscherm wordt getoond.

Let op! Om je EM4450 snel te kunnen configureren voor verbinding met het Internet, dien je vooraf vast te stellen welke verbindingsmethode je provider gebruikt ('DHCP', 'PPPoE', 'Static IP' of 'PPtP'). Je vindt deze gegevens in de informatiegegevens die je van je provider hebt ontvangen.

6.2 Configuratie voor een DHCP verbinding

1. Klik links in het menu op 'Network'.
2. Klik links in het menu op 'WAN'.

3. Selecteer ‘Dynamic IP’.
4. Typ in het veld ‘Hostname’ de hostname die je van je provider hebt ontvangen. Voorbeeld van een hostname:’CC1234567-a’. (Alleen bij een @Home internet verbinding).
5. Klik links in het menu op ‘MAC Clone’. (Alleen van toepassing indien je een provider hebt met Mac-adres registratie.)
6. Klik op de knop ‘Clone MAC Adress’.
7. Klik op ‘Save’.
8. Sluit je internetbrowser.
9. Je beschikt binnen 5 minuten over een werkende internet verbinding.

Tip! Als je een kabelprovider gebruikt zoals @home, kijk dan bij hoofdstuk 11 als je niet binnen 5 minuten een werkende verbinding tot stand kon brengen.

6.3 Configuratie voor een Static IP internet verbinding

1. Klik links in het menu op ‘Network’.
2. Klik links in het menu op ‘WAN’.
3. Selecteer ‘Static IP’.
4. Typ in het veld ‘IP Address’ het IP adres dat je van je provider hebt ontvangen.
5. Typ in het veld ‘Subnet Mask’ het subnet masker dat je van je provider hebt ontvangen.
6. Typ in het veld ‘Default Gateway’ het gateway adres dat je van je provider hebt ontvangen.
7. Typ in het veld ‘Primary DNS’ het primaire DNS adres dat je van je provider hebt ontvangen.
8. Typ in het veld ‘Secondary DNS’ het secundaire DNS adres dat je van je provider hebt ontvangen. Indien je geen secundair DNS adres hebt ontvangen laat je dit veld leeg.
9. Klik op ‘Save’.
10. Sluit je internetbrowser.
11. Je beschikt binnen 5 minuten over een werkende internet verbinding.

6.4 Configuratie voor een PPPoE internet verbinding

1. Klik links in het menu op ‘Network’.
2. Klik links in het mneu op ‘WAN’.
3. Selecteer ‘PPPoE’.
4. Typ in het veld ‘User Name’ de gebruikersnaam dat je van je provider hebt
5. ontvangen.
6. Typ in het veld ‘Password’ het wachtwoord dat je van je provider hebt
7. ontvangen.
8. Klik op ‘Save’.
9. Sluit je internetbrowser.
10. Je beschikt binnen 5 minuten over een werkende internet verbinding.

6.5 Configuratie voor een PPtP internet verbinding

1. Klik links in het menu op ‘Network’.
2. Klik links in het menu op ‘WAN’.
3. Selecteer ‘PPtP’.
4. Typ in het veld ‘User Name’ de gebruikersnaam die je van je provider hebt
5. ontvangen.
6. Typ in het veld ‘Password’ het wachtwoord dat je van je provider hebt
7. ontvangen.
8. Typ in het veld ‘Server IP Address/Name’ het gateway adres voor je ADSL modem in. (Voor Speedtouch Home modems is dit standaard 10.0.0.138).
9. Typ in het veld ‘IP Address’ het IP adres voor je ADSL modem in. (Voor Speedtouch Home modems is dit standaard 10.0.0.150).
10. Typ in het veld ‘Subnet Mask’ het subnetmasker van je ADSL modem in. (Voor Speedtouch Home modems is dit standaard 255.255.255.0).
11. Typ in het veld ‘Gateway’ het gateway adres van je ADSL modem in. (Voor Speedtouch Home modems is dit standaard 10.0.0.138.)
12. Klik op ‘Save’.
13. Sluit je internetbrowser.
14. Je beschikt binnen 5 minuten over een werkende internet verbinding.

7.0 Draadloze beveiliging instellen

Omdat ook onbevoegden het signaal van een draadloos netwerk kunnen ontvangen, wordt je aanbevolen om je netwerk te beveiligen. Er zijn verschillende methodes die je kunt gebruiken om je netwerk te beveiligen.
Om een methode toe te passen in een netwerk, is het noodzakelijk dat alle draadloze netwerkapparatuur deze methode ondersteunt. De sterkste vorm van draadloze beveiliging is WPA (WiFi Protected Access).

De makkelijkste manier om je draadloze netwerk te beveiligen is met behulp van de installatiewizard, zoals hieronder staat beschreven. Indien je bij de installatie van de EM4450 geen gebruik wilt maken van de wizard op de meegeleverde cd-rom, kun je de beveiliging ook handmatig instellen. Zie hiervoor hoofdstuk 8

1. Schakel je computer in.
2. Plaats de cd-rom in de cd-rom speler.
3. De wizard wordt gestart.
4. Selecteer je taal, en klik op ‘Next’.
5. Selecteer ‘Draadloze beveiliging instellen’ en klik op ‘Volgende’.
6. Volg de stappen op het scherm totdat de installatie voltooid is. Je hebt nu een beveiligd draadloos netwerk.

Let op! WPA beveiliging wordt ondersteund vanaf Windows 2000. Dit type beveiliging kan dus niet gebruikt worden onder Windows 98 en ME! Heb je geen Windows Vista, XP of Windows 2000, gebruik dan WEP beveiliging.

8.0 Beveiliging handmatig instellen in de router

Je kunt behalve via de cd, de beveiliging ook handmatig instellen. In het komende hoofdstuk gaan we uitleggen hoe dit gedaan moet worden. Eminent beveelt de WPA encryptie aan omdat dit momenteel de meest veilige beveiligingsmethode is.

8.1 WPA beveiliging handmatig instellen via de router

1. Schakel je computer in.
2. Open je internetbrowser (Bijvoorbeeld Internet Explorer, Netscape of Firefox).
3. Maak de adresbalk leeg, en tik dan het volgende in: http://192.168.1.1
4. Druk op de entertoets of klik op ‘Ga naar’.
5. Typ ‘admin’ bij gebruikersnaam.
6. Typ ‘admin’ bij wachtwoord.
7. Klik op ‘Ok’.
8. Het openingsscherm wordt getoond.
9. Klik links in het menu op ‘Wireless’.
10. Klik links in het menu op ‘Wireless Settings’.
11. Plaats een vinkje bij ‘Enable Wireless Security’.
12. Selecteer bij ‘Security Type’ het gewenste beveiligingstype, in dit geval WPA-PSK/WPA2-PSK
13. Bij ‘Security Option’ kies je WPA-PSK.
14. Bij ‘Encryption’ kies je TKIP.
15. Nu ga je naar ‘PSK Passphrase’. In dit scherm kun je je gewenste beveiligingscode invullen. Hierbij kun je naar willekeur cijfers en letters gaan gebruiken. Hou er wel rekening mee dat een WPA beveiliging minimaal 8 tekens moet bevatten, maximaal 63 tekens. Noteer deze code.
16. Klik op ‘Save’.
17. Klik op ‘Ok’, dan nogmaals op ‘OK’. De router zal nu de instellingen gaan opslaan.

8.2 WEP beveiliging handmatig instellen via de router

1. Schakel je computer in.
2. Open je internetbrowser (Bijvoorbeeld Internet Explorer, Netscape of Firefox).
3. Maak de adresbalk leeg, en tik dan het volgende in: http://192.168.1.1
4. Druk op de entertoets of klik op ‘Ga naar’.
5. Typ ‘admin’ bij gebruikersnaam.
6. Typ ‘admin’ bij wachtwoord.

7. Klik op ‘OK’.
8. Het openingsscherm wordt getoond.
9. Klik links in het menu op ‘Wireless’.
10. Klik links in het menu op ‘Wireless Settings’.
11. Plaats een vinkje bij ‘Enable Wireless Security’.
12. Selecteer bij ‘Security Type’ het gewenste beveiligingstype, in dit geval WEP.
13. Selecteer nu het Key Type: Je kunt kiezen uit 64bit, 128bit.
14. Vul bij 64bit beveiliging een wachtwoord in van exact tien tekens. Dit mogen zowel cijfers als letters zijn. Kies je letters, dan mag je A t/m F gaan gebruiken. Gebruik je 128bit beveiliging, dan dient je code exact 26 tekens te bevatten. Ook hier mag je zowel cijfers als letters gebruiken. Kies je letters, dan mag je A t/m F gaan gebruiken.
15. Deze net ingestelde code heb je later nog nodig. Schrijf deze code dus op.
16. Klik op ‘Save’.
17. Klik op ‘OK’. Dan nogmaals op ‘OK’. De router zal nu de instellingen gaan opslaan.

Let op! Eminent raadt aan de beveiliging in te stellen wanneer je de router bekabeld op de PC hebt aangesloten. .

Noteer hier het type beveiliging dat je hebt ingesteld, de netwerknaam en het wachtwoord:

☐ *WPA* ☐ *WEP*

Netwerknaam: _____

Wachtwoord: _____

8.3 WPA/WPA2 met Radius beveiliging handmatig instellen via de router

De EM4450 beschikt ook over de mogelijkheid om een WPA/WPA2 beveiliging op te zetten via een zogenaamde Radius Server. Dit is een beveiligingstype welke alleen in een bedrijfsomgeving met een eigen Radius-server wordt gebruikt.

9.0 Het draadloze netwerk op de PC instellen.

Nu de router is beveiligd moet nu de PC zelf worden ingesteld zodat deze het beveiligde draadloze netwerk herkend, en kan verbinden.
Windows XP en Windows Vista zijn momenteel de meest gebruikte besturingssystemen. We gaan uitleggen hoe je een draadloze verbinding onder deze systemen kunt opzetten.

Tip: Nadat de router is ingesteld met een WEP of WPA beveiliging, kun je de netwerkkabel van de PC halen, alvorens met stap 9.1 te beginnen.

9.1 Draadloos netwerk onder Windows XP instellen.

Om de draadloze verbinding tot stand te brengen onder Windows XP dien je de volgende stappen uit te voeren:

1. Start je PC op.
2. Klik op ‘Start’.
3. Ga naar ‘Configuratiescherm’.
4. Selecteer in het configuratiescherm ’Netwerkverbindingen’.
5. Als het goed is, zie je nu je draadloze kaart of adapter staan. Klik deze met de rechtermuisknop aan.
6. Kies nu voor ‘Beschikbare draadloze netwerken weergeven’. Er wordt nu een lijst getoond met aanwezige draadloze netwerken.
7. In het lijstje met beschikbare draadloze netwerken selecteer je het eigen netwerk.
8. Wanneer je nu kiest voor ‘verbinding maken’ gaat je PC een waarschuwing geven dat dit netwerk is beveiligd, en dat er een netwerksleutel is vereist.
9. Vul nu de beveiligingssleutel in, en kies voor ‘verbinding maken’.
10. Is je sleutel goed ingevoerd, dan zal Windows na enige tijd aangeven dat het netwerk is verbonden. Je kunt nu online.

9.2 Draadloos netwerk onder Windows Vista instellen.

Om de draadloze verbinding tot stand te brengen onder Windows Vista dien je de volgende stappen uit te voeren:

1. Klik ‘Start’.
2. Klik nu op het ‘Configuratiescherm’.
3. Kies hier voor ‘Netwerk en Internet’.
4. Ga naar het ‘Netwerkcentrum’.
5. Aan de linkerzijde van het verschenen menu kies je voor ‘Draadloos netwerk beheren’.
6. In dit venster kies je voor ‘Toevoegen’
7. In het volgende scherm kies je dan voor ‘Een draadloos netwerk binnen bereik van deze PC toevoegen’.
8. In het nieuwe venster kies je het eigen netwerk.
9. Klik nu op ‘Verbinding maken’.
10. Je PC zal nu de volgende melding geven: “Geef een sleutel voor de netwerkbeveiliging of wachtwoordzin op voor het netwerk.”
    Vul hier dan je beveiligingssleutel in.
11. Kies nu voor ‘Verbinding maken’. Indien je sleutel correct is ingevuld, zal je PC nu een draadloze verbinding hebben, en ben je online.

10.0 Controle over de internetverbinding

De EM4450 beschikt over een geavanceerde firewall. Hiermee heb je bijna volledige controle over de internetverbinding. De firewall laat je toe om instellingen te maken waarmee je computers voor een bepaalde tijd verbiedt om een op internet te komen. Ook kun je websites blokkeren. Dit kan tijdelijk, permanent, of tussen bepaalde uren, bijvoorbeeld tijdens werkuren.

10.1 Firewall inschakelen

Om de juiste instellingen in de firewall te maken, gaan we deze eerst inschakelen. Volg daarvoor de volgende stappen:

1. Open je internetbrowser (Bijvoorbeeld Internet Explorer, Netscape of Firefox).
2. Maak de adresbalk leeg, en tik dan het volgende in: http://192.168.1.1
3. Druk op de entertoets of klik op ‘Ga naar’.
4. Typ ‘admin’ bij gebruikersnaam. Typ ‘admin’ bij wachtwoord.
5. Klik op ‘OK’.
6. Het openingsscherm wordt getoond.
7. Klik aan de linkerzijde van het scherm onder ‘Advanced Settings’ op ‘Security’.
8. In het veld dat nu wordt geopend zet je een vinkje bij ‘Enable Firewall’.
9. Klik op ‘Save’.
10. De firewall in nu ingeschakeld.

10.2 Internettoegang verbieden via IP-adressen

De firewall stelt je in staat om aan de hand van het IP-adres een PC de toegang tot internet te verbieden. Om deze optie te gebruiken, moet de optie ‘IP-adres filtering’ ingeschakeld zijn. Om deze optie in te schakelen, volg je dezelfde stappen als in hoofdstuk 10.1. Echter, nu zet je bij stap 8 een vinkje bij ‘Enable IP-Adress Filtering’. Volg dan de stappen 9 en 10.

1. Klik in het linkerscherm onder ‘Advanced Settings’ op de optie ‘IP Adress Filtering’.
2. In het volgende scherm klik je op ‘Add New’.
3. In het scherm wat je nu ziet kun je de gegevens invullen.
4. Klik in het veld ’Effective time’.

In dit veld kun je de gewenste tijd ingeven dat een PC niet online mag komen. Wil je dat een PC van 10 uur ’s ochtends tot 8 uur ’s avonds niet online mag komen, dan vul je in het eerste vakje van ‘Effective time’ 1000 in. In het tweede vakje vul je dan 2000 in.

5. Bij ‘Lan IP Adress’ vul je dan het IP-adres in van de PC waarvan je de toegang wilt weigeren op de ingegeven tijden. Bijvoorbeeld ‘ 192.168.1.5’.

6. Bij ‘Action’ kies je dan voor ‘Deny’.
7. Klik nu op ‘Save’.
8. Op de opgegeven tijden is toegang tot het internet nu onmogelijk voor de pc met het door jou opgegeven IP-adres.

Tip: In hoofdstuk 11 wordt uitgelegd hoe je het IP-adres van een computer kunt opvragen..

10.3 Toegang tot internet verbieden met ‘Domain Filtering’.

Met de EM4450 is het mogelijk om bepaalde domeinen of websites niet toe te staan. Wil je bijvoorbeeld dat je zoon of dochter niet op bepaalde sites mag komen, dan kan je dat instellen. Om deze optie in te schakelen, volg je dezelfde stappen als in hoofdstuk 10.1. Echter, nu zet je bij stap 8 een vinkje bij ‘Enable Domain Filtering’. Volg dan de stappen 9 en 10.

1. Klik nu in het linkerscherm op ‘Domain Filtering’.
2. Klik op ‘Add New’.
3. Klik in het veld ’Effective time’.

In dit veld kun je de gewenste tijd ingeven dat een PC niet online mag komen. Wil je dat een PC van 10 uur ’s ochtends tot 8 uur ’s avonds niet online mag komen, dan vul je in het eerste vakje van ‘Effective time’ 1000 in. In het tweede vakje vul je dan 2000 in.

4. Bij ‘Domain Name’ kun je ingeven welk Domein of website niet mee bezocht mag worden gedurende de ingestelde tijd. Wil je bijvoorbeeld niet dat iemand op de opgegeven tijd naar www.google.nl gaat, dan vul je deze sitenaam in bij ‘Domain Name’.
5. In het veld ‘Status’ dient ‘Enabled’ actief te staan.
6. Klik nu op ‘Save’.
7. Op de opgegeven tijden zijn de opgeven domeinen of websites nu niet meer toegestaan.

10.4 Internet verbieden via ‘MAC Address Filtering’

Behalve de eerder genoemde mogelijkheden om beperkingen te stellen aan internettoegang, is er nog een andere mogelijkheid om de internettoegang te blokkeren. Deze methode is ook direct het meest effectief. De volledige toegang tot internet wordt hiermee geblokkeerd, en je hoeft geen tijden in te geven. Om deze optie in te schakelen, volg je dezelfde stappen als in hoofdstuk 10.1. Nu zet je bij stap 8 een vinkje bij ‘Enable Mac-address filtering’. Volg dan de stappen 9 en 10.

1. Klik in het linkerscherm op ‘ MAC Filtering’.

2. In het volgende scherm klik je op ‘Add New’.
3. Bij ‘ MAC Address’ vult je het gewenste Mac adres in.
4. Bij ‘Description’ kun je een beschrijving geven. Hier kun je bijvoorbeeld de naam invullen van degene die niet meer online mag.
5. In het veld ‘Status’ dient ‘Enabled’ actief te staan.
6. Klik nu op ‘Save’.
7. Vanaf nu is de toegang tot het internet volledig geblokkeerd voor het opgegeven Mac-adres.

Tip: In hoofstuk 11 wordt uitgelegd hoe je het Mac-adres van een computer kunt opvragen.

11.0 Vraag & antwoord

V: Ik krijg de melding ‘ Het IP-adres van de netwerkkaart staat verkeerd’. Wat nu?
A: Deze melding verschijnt in beeld wanneer de PC geen juist IP-adres heeft ontvangen van de router. Controleer of alle kabels goed aangesloten zijn, reset de EM4450 en probeer het opnieuw. Bij voorkeur dien je de router bekabeld (dus niet draadloos) in te stellen. Wanneer de verbinding bekabeld tot stand is gebracht, kun je de draadloze verbinding gaan instellen zoals in de handleiding is aangegeven.

V: Ik heb de router ingesteld. Alles gaat goed, behalve de toegang tot het internet. Mijn provider is Chello.
A: Zorg ervoor dat het juiste Mac-adres tijdens het instellen is geselecteerd. Wanneer het verkeerde Mac-adres is geselecteerd, krijg je deze melding.

V: Ik heb de router ingesteld. Alles gaat goed, behalve de toegang tot het internet. Mijn provider is Chello/@Home/Casema of een andere DHCP provider.
A: In een aantal gevallen kan het gebeuren dat de modem geen internettoegang aan de router kan bieden. De volgende stappen kun je volgen om de verbinding alsnog werkend te krijgen:
1. Zet de router en modem uit.
2. Wacht ongeveer 10 minuten.
3. Zet de modem aan, wacht totdat deze volledig opgestart is, zet dan de router aan, en laat deze ook volledig opstarten.
4. De verbinding zal nu moeten werken.

V: Ik heb de vorige oplossing geprobeerd, maar het internet werkt nog niet. Wat moet ik doen?
A: Er is nog een andere methode:
1. Log in op de routerpagina via http://192.168.1.1
2. Gebruikersnaam: admin, Wachtwoord:admin
3. Je bent nu ingelogd in het hoofdscherm van de EM4450.
4. Draai nu de coaxkabel van je modem los.
5. Op de routerpagina klik je onder ‘WAN’ op ‘Renew’

6. Er verschijnt nu een IP-adres van je modem in het scherm. Vaak is dit volgend adres: 192.168.100.x
7. Draai nu de coaxkabel weer op je modem, en wacht todat het Online/Internet ledje weer gaat branden.
8. Klik nu in het routerscherm weer op 'Renew'.
9. Als het goed is verschijnt er nu het IP-adres dat door je provider wordt verstrekt in je scherm. In dat geval heb je een internetverbinding.

V: Ik wil weten wat mijn IP-adres is. Hoe vraag ik deze op?
A: Om het IP-adres te achterhalen, voer je de volgende stappen uit.

Stappen voor Windows XP/2000 en Windows Vista:
1. Klik op 'Start'.
2. Ga naar 'uitvoeren'.
3. Vul hier in: 'cmd'.
4. Druk op de entertoets of klik op 'OK'.
5. Vul nu in: ipconfig'.
6. Druk weer op de entertoets.
7. Je ziet nu het IP-adres staan.

Stappen voor Windows98/ME:
1. Klik op 'Start'.
2. Ga naar 'uitvoeren'.
3. Vul hier in 'winipcfg'.
4. Druk op de entertoets of klik op 'OK'.
5. Je ziet nu het IP-adres of het Automatisch persoonlijk adres staan.

V: Ik wil graag het Mac-adres van mijn netwerkkaart weten. Hoe kom ik deze te weten?
A: Om het Mac-adres van je netwerk te achterhalen kun je de volgende stappen achterhalen:

Stappen voor Windows XP/2000 en Windows Vista:
1. Klik op 'Start'.
2. Ga naar 'uitvoeren'.
3. Vul hier in: 'cmd'.
4. Druk op de entertoets of klik op 'OK'.
5. Vul nu in: 'ipconfig /all'.
6. Druk weer op de entertoets.
7. Je ziet nu het 'fysieke adres' staan. Dit is het Mac-adres van je netwerkkaart.

Stappen voor Windows98/ME:
1. Klik op 'Start'.
2. Ga naar 'uitvoeren'.
3. Vul hier in 'winipcfg'.

4. Druk op de entertoets of klik op ‘OK’.
5. Je ziet nu het ‘adapteradres’ ofwel het Mac-adres staan van je netwerkkaart.

V: Hoe reset ik de EM4450?
A: Je reset de EM4450 door eerst de stroomstekker van de router te halen. Dan druk je een paperclip op de resetknop. Doe dan de stroomstekker weer in de EM4450, blijf intussen met de paperclip het resetknopje indrukken. Op de router gaat het ledje ‘Sys’ branden. Wacht totdat deze weer gaat knipperen, haal de paperclip van de resetknop. De EM4450 is nu gereset, en staat weer op fabrieksinstellingen.

12.0 Service en ondersteuning

Deze handleiding is door de technische experts van Eminent met zorg opgesteld. Mocht je desondanks problemen ervaren bij de installatie of in het gebruik van je Eminent product, dan kun je een email sturen naar support@eminent-online.com. Je kunt tevens gebruik maken van het Eminent servicenummer. Bel 0900-EMINENT (0900-3646368). Vlaamse gebruikers bellen 0900-70090. Bel je met je mobiele telefoon dan betaal je 45ct per minuut exclusief de kosten voor het gebruik van je mobiele telefoon.

Eminent Advanced Manual

Inhoudsopgave

Waarom een Eminent Advanced Manual?

Eminent heeft de Eminent Advanced Manual speciaal ontwikkeld voor uw gemak! De Eminent Advanced Manual stelt u in staat om de geavanceerde mogelijkheden van uw thuisnetwerk te ontdekken. Zo helpt de Eminent Advanced Manual u bijvoorbeeld op weg bij het instellen van uw firewall zodat u te allen tijde beschikt over optimale beveiliging van uw eigen netwerk. Natuurlijk komt ook de beveiliging van uw draadloze netwerk uitgebreid aan bod. Met de Eminent Advanced Manual beschikt u over een schat aan informatie en over een handig naslagwerk. Zo beschikt u op een eenvoudige manier over functies die voorheen enkel beschikbaar waren voor professionele en ver gevorderde gebruikers.

Uw tips en suggesties in de Eminent Advanced Manual?

De Eminent Advanced Manual is tot stand gekomen in samenwerking met een aantal tevreden Eminent gebruikers. Wilt u graag dan een bepaalde optie wordt opgenomen in de Eminent Advanced Manual of heeft u suggesties of tips met betrekking tot de Eminent Advanced Manual dan kunt u een bericht sturen naar communications@eminent-online.com. Uw tips en suggesties zullen worden verzameld en worden verwerkt in de nieuwe editie van de Eminent Advanced Manual.

Service en ondersteuning

De Eminent Advanced Manual is met zorg opgesteld door gebruikers en technische experts van Eminent. Mocht u desondanks problemen ervaren bij de installatie of in het gebruik van uw Eminent product, dan kunt u een bericht sturen naar support@eminent-online.com.

U kunt tevens gebruik maken van het Eminent servicenummer. Bel 0800-EMINENT (0800-3646368). Vlaamse gebruikers bellen 0800-50150. Met uw mobiele telefoon belt u 0900-EMINENT (0900-3646368) of, in geval u woonachtig bent in Vlaanderen 0900-70090. 45ct per minuut exclusief de kosten voor het gebruik van uw mobiele telefoon.

Netwerkinstellingen voor Windows 98 en ME

1. Voor Windows 98: Klik met de rechter muisknop op ‘Netwerkomgeving’ op je bureaublad.
2. Voor Windows ME: Klik met de rechter muisknop op ‘Mijn netwerklocaties’ op je bureaublad.
3. Kies ‘Eigenschappen’.
4. Selecteer ‘TCP/IP’ van je netwerkkaart.

5. Klik op ‘Eigenschappen’.
6. Kies ‘Automatisch een IP adres verkrijgen’.
7. Klik op het tabblad ‘WINS configuratie’.
8. Kies ‘WINS omzetting uitschakelen’.
9. Klik op tabblad ‘DNS configuratie’.
10. Kies ‘DNS uitschakelen’.
11. Klik op tabblad ‘Gateway’.
12. Verwijder eventueel geïnstalleerde gateways.
13. Klik op ‘Ok’.
14. Klik op ‘Ok’ in het scherm ‘Netwerk’.
15. Start je computer opnieuw op.
16. Klik op ‘Start’.
17. Klik op ‘Uitvoeren’.
18. Type ‘winipcfg’.
19. Klik op ‘Ok’.
20. Windows toont je het scherm ‘IP configuratie’.
21. Selecteer de op het Eminent apparaat aangesloten Ethernet adapter (netwerkkaart).
22. Klik op ‘Alle vrijgeven’.
23. Klik op ‘Alle vernieuwen’.
24. Klik op ‘Ok’.

Netwerkinstellingen voor Windows 2000 en XP

1. Klik met de rechter muisknop op ‘Mijn netwerklocaties’ op je bureaublad.
2. Kies ‘Eigenschappen’.
3. Klik met de rechter muisknop op ‘LAN-verbinding’.
4. Kies ‘Eigenschappen’.
5. Selecteer ‘internet protocol (TCP/IP)’.
6. Klik op ‘Eigenschappen’.
7. Kies ‘Automatisch een IP adres laten toewijzen’.
8. Kies ‘Automatisch een DNS serveradres laten toewijzen’.
9. Klik op ‘Ok’.
10. Windows toont het scherm ‘Eigenschappen voor LAN-verbinding’.
11. Klik op ‘Ok’.
12. Windows 2000: Sluit het scherm ‘Netwerk- en inbelverbindingen’.
13. Windows XP: Sluit het scherm ‘Netwerkverbindingen’.
14. Start je computer opnieuw op.
15. Klik op ‘Start’.
16. Klik op ‘Uitvoeren’.
17. Type ‘cmd’.
18. Druk op de entertoets.
19. Type ‘ipconfig /release’.

20. Druk op de entertoets.
21. Type ‘ipconfig /renew’.
22. Druk op de entertoets.
23. Type ‘exit’.
24. Druk op de entertoets.

Het instellen van Internet Explorer 5 en 5.5

1. Start je Internet Explorer.
2. Klik op ‘Stop’ of wacht tot er wordt aangegeven dat de pagina niet kan worden gevonden.
3. Als je wordt gevraagd om verbinding te maken kun je dit annuleren.
4. Klik op ‘Extra’.
5. Klik op ‘internet-opties’.
6. Klik op het tabblad ‘Verbindingen’.
7. Klik op ‘LAN-instellingen’.
8. Schakel het vinkje bij ‘Instellingen van Internet Explorer automatisch vinden’ aan.
9. Schakel het vinkje bij ‘Automatisch configuratie script gebruiken’ uit.
10. Schakel het vinkje bij ‘Proxy server gebruiken’ uit.
11. Klik op ‘Ok’.
12. Verwijder eventuele inbelverbindingen met de knop ‘Verwijderen’.
13. Klik op ‘Instellingen’ (helemaal bovenaan) om de wizard internet te starten.
14. Kies de laatste optie (Ik wil verbinding maken via een LAN netwerk).
15. Klik op ‘Volgende’.
16. Selecteer ‘Ik maak een verbinding via een LAN netwerk’.
17. Klik op ‘Volgende’.
18. Plaats een vinkje bij ‘Proxyserver automatisch opsporen’.
19. Klik op ‘Volgende’.
20. Selecteer ‘Nee’.
21. Klik op ‘Volgende’.
22. Klik op ‘Voltooien’.
23. Sluit alle vensters en herstart je pc.

Het instellen van Internet Explorer 6

1. Start je Internet Explorer.
2. Klik op ‘Stop’ of wacht tot er wordt aangegeven dat de pagina niet kan worden gevonden.
3. Als je wordt gevraagd om verbinding te maken kun je dit annuleren.
4. Klik op ‘Extra’.
5. Klik op ‘internet-opties’.
6. Klik op het tabblad ‘Verbindingen’.
7. Klik op ‘LAN-instellingen’.
8. Schakel het vinkje bij ‘Instellingen van Internet Explorer automatisch vinden’ aan.

9. Schakel het vinkje bij ‘Automatisch configuratie script gebruiken’ uit.
10. Schakel het vinkje bij ‘Proxy server gebruiken’ uit.
11. Klik op ‘Ok’.
12. Verwijder eventuele inbelverbindingen met de knop ‘Verwijderen’.
13. Klik op ‘Instellingen’ (helemaal bovenaan) om de ‘Wizard Nieuwe verbinding’ te starten.
14. Klik op ‘Volgende’.
15. Selecteer ‘Verbinding met het internet maken’.
16. Klik op ‘Volgende’.
17. Selecteer ‘Ik wil handmatig een verbinding instellen’.
18. Klik op ‘Volgende’.
19. Selecteer ‘Verbinding maken via een permanente breedband verbinding’.
20. Klik op ‘Volgende’.
21. Klik op ‘Voltooien’.
22. Sluit alle vensters en herstart je pc.

DHCP, het automatisch toekennen van IP adressen

Voor de ontwikkeling van DHCP (Dynamic Host Configuration Protocol) werden TCP/IP instellingen met de hand geconfigureerd op iedere TCP/IP cliënt (zoals bijvoorbeeld uw computer). Dit kan een lastig karwei zijn wanneer het een groot netwerk betreft of als er regelmatig iets moet worden veranderd in het netwerk. Om het altijd opnieuw te moeten instellen van een IP-adres te vermijden werd DHCP ontwikkeld. Met DHCP worden IP-adressen automatisch toegekend wanneer nodig, en vrijgegeven als ze niet langer nodig zijn. Een DHCP server heeft een reeks (‘pool’) van geldige adressen die hij kan toekennen aan de cliënt. Wanneer een cliënt bijvoorbeeld opstart zal deze een bericht versturen met het verzoek voor een IP-adres. Een DHCP server (er kunnen er meerdere zijn in een netwerk) antwoord door IP-adres en configuratiegegevens terug te sturen. De cliënt zal een bevestiging van ontvangst versturen waarna de cliënt kan deelnemen aan het netwerk.

Het vertalen van IP-adressen en domeinnamen

IP-adressen zijn verre van gebruiksvriendelijk. Domeinnamen daarentegen zijn eenvoudiger te onthouden en te gebruiken. Het proces waarin een domeinnaam wordt vertaald in een voor een machine (zoals uw computer) begrijpelijk adres wordt ‘name resolution’ genoemd. Het voornoemde proces wordt uitgevoerd door een ‘Domain Name System’ server. Dankzij DNS gebruikt u domeinnamen in plaats van IP-adressen als u een website bezoekt of een emailbericht verstuurd.
Een aan DNS verwante optie is Dynamic DNS of DDNS. Wanneer uw provider werkt met dynamische IP-adressen (‘dynamisch’ betekent in deze dat de IP-adressen

frequent wijzigen) en wilt u toch uw IP-adres aan een domeinnaam koppelen dan doet u dit middels DDNS. Immers; wanneer uw provider uw IP-adres verandert dan wijzigt ook het IP-adres waarnaar uw domeinnaam verwijst. Om Dynamic DNS te kunnen gebruiken dient u zich te registeren bij een Dynamic DNS provider zoals 'www.dyndns.org' en 'www.no-ip.com'.

Een enkel publiek IP-adres gebruiken voor uw gehele netwerk

Network Address Translation (NAT) is een internetstandaard waarmee een lokaal netwerk gebruik kan maken van privé IP-adressen. Privé IP-adressen zijn adressen die worden gebruikt binnen het eigen netwerk. Privé IP-adressen worden niet op het internet herkend, noch gebruikt. Een IP-adres dat op internet wordt gebruikt wordt ook wel een publiek IP-adres genoemd.

NAT stelt u in staat een enkel publiek IP-adres te delen met meerdere computers in uw netwerk. NAT zorgt ervoor dat de computers in uw netwerk zonder problemen gebruik kunnen maken van het internet. Gebruikers op het internet echter, hebben geen toegang tot de computers in uw netwerk. U begrijpt dat NAT, mede dankzij het feit dat de privé IP-adressen niet zichtbaar zijn op het internet, tevens een bepaalde mate van beveiliging biedt. Gelukkig maken de meeste routers tegenwoordig gebruik van NAT.

Beveiliging voor uw computer en uw netwerk

Een firewall kan bestaan uit zowel een software- of een hardwarematige oplossing en plaatst als het ware een muur tussen het interne netwerk en de buitenwereld. Firewalls controleren in de regel zowel inkomend als uitgaand dataverkeer. Firewalls kunnen worden ingesteld om bepaalde informatie vanaf het internet tegen te houden of door te laten. Ook kunnen firewalls worden ingesteld om aanvragen van binnenuit tegen te houden of door te laten. Om een firewall in te stellen worden 'regels', 'rules' of 'policies' gebruikt. Deze geven aan wat een firewall moet tegenhouden of juist moet doorlaten en vormen dus het eigenlijke filter.
De meeste routers zijn voorzien van diverse firewall-functies. Het grote voordeel van een firewall in een router (hardwarematige oplossing) is dat een aanval van buitenaf al wordt afgeslagen voordat uw netwerk wordt bereikt. Wilt u gebruik maken van een softwarematige firewall dan kunt u bijvoorbeeld de in Windows XP Service Pack 2 ingebouwde firewall gebruiken, betere alternatieven zijn het gratis beschikbare ZoneAlarm en de commerciële pakketten Norman, Norton, Panda en McAfee. Deze commerciële pakketten bieden desgewenst ook bescherming tegen virussen.

Een computer binnen uw netwerk beschikbaar stellen voor internetgebruikers

De DMZ of DeMilitarized Zone vormt de zone tussen de buitenwereld – het internet – en het veilige, interne netwerk. De computer die in de DMZ geplaatst wordt, is bereikbaar vanaf het internet. Dit in tegenstelling tot de computers die zich buiten de DMZ bevinden en dus veilig zijn. De DMZ wordt dan ook vaak gebruikt voor servers die websites hosten. Websites moeten immers toegangkelijk zijn vanaf het internet. Ook wanneer men veelvuldig online games speelt plaatst men een computer vaak in een DMZ. Het verdient echter aanbeveling om, wanneer u een computer in de DMZ plaatst, toch een softwarematige firewall (zoals bijvoorbeeld het gratis beschikbare ZoneAlarm) te installeren. Dit omdat de firewall alle poorten van de router opent voor een computer binnen de DMZ. Er is dus geen enkele restrictie op dataverkeer, terwijl dit in sommige situaties toch wenselijk is.

Net als de DMZ functie stelt ook Virtual Server u in staat een computer binnen uw netwerk, ingericht als bijvoorbeeld FTP- of webserver, toegangkelijk te maken vanaf het internet. U kunt, wanneer u gebruik maakt van een Virtual Server, poorten opgeven die in de firewall moeten worden geopend. Dit is tevens het belangrijkste verschil met de DMZ: wanneer u een computer in de DMZ plaatst worden alle poorten voor de betreffende computer geopend. Gebruikt u Virtual Server dan kunt u enkel de poorten die voor het gebruik van de betreffende computer van belang zijn openen.

Port Triggering oftewel Special Apps is gebaseerd op hetzelfde principe als Virtual Server. Ook Port Triggering stelt u in staat een computer binnen uw netwerk, ingericht als bijvoorbeeld FTP- of webserver, toegangkelijk te maken vanaf het internet. Wanneer u gebruik maakt van Virtual Server, dan blijven de door u toegewezen poorten te allen tijde geopend. Bij Port Triggering echter, worden de betreffende poorten alleen geopend als de betreffende applicatie daarom vraagt.

Het vereenvoudigen van netwerkbeheer

UPnP ‘Universal Plug and Play’: de naam doet vermoeden dat UPnP erg lijkt op het bekende – en beruchte – ‘Plug & Play’. Niets is minder waar. UPnP is een heel andere techniek. De insteek is dat UPnP apparaten in staat moeten zijn via TCP/IP met elkaar te communiceren ongeacht het besturingssysteem, de programmeertaal en de hardware. UPnP dient het leven van de gebruiker aanzienlijk makkelijker te maken. Naast de producten van een beperkt aantal andere fabrikanten, ondersteunen de meeste netwerkproducten van Eminent UPnP. Meer informatie over UPnP vindt u op de navolgende website: ‘www.upnp.org’.

Websites met expliciete inhoud blokkeren

Parental Control stelt u in staat een of meerdere computers binnen uw netwerk de toegang tot het internet te ontzeggen. Parental Control bestaat veelal uit meerdere functies zoals bijvoorbeeld ‘URL Blocking’. Deze functie blokkeert websites middels zogenaamde ‘Key Words’ of steekwoorden. Websites met expliciete inhoud worden zo geblokkeerd. Vaak wordt ‘URL Blocking’ gecombineerd met tijd en/of datum blokkades. Dergelijke blokkades stellen u in staat internettoegang per tijdseenheid toe te laten of juist tegen te houden. Om uw eigen schema van blokkades op te stellen maakt u gebruik van ‘rules’, ‘regels’ of ‘policies’ (zie ook ‘Schedule Rule’). Deze ‘regels’ beschrijven precies wanneer en waarop een bepaalde actie, in dit geval een blokkade, moet worden toegepast.

Dataverkeer op pakketniveau controleren

Het pakketfilter (of ‘Packet Inspection’) is een programma dat datapakketten controleert terwijl ze passeren. Dit intelligente pakketfilter controleert de passerende datastroom of bedrijfsspecifieke definities zoals het IP- of gebruikersadres, tijd en datum, functie en tal van andere definities. Het pakketfilter is het best voor te stellen als een portier. De portier screent de voorbijgangers: “wie bent u en wat is uw bestemming?” De voorbijgangers die de portier als onveilig of onbetrouwbaar beschouwd worden tegengehouden.

In de meeste apparatuur hoeft u het pakketfilter niet te configureren. U hoeft de optie slechts in te schakelen. Het gebruik van deze optie wordt dan ook beslist aangeraden.

Een compleet domein blokkeren

Een domeinfilter of ‘Domain Filter’ stelt u in staat een compleet domein te blokkeren. Een domein is een locatie op Internet zoals een website. Een ‘Domain Filter’ vertoont dus grote gelijkenis met een ‘URL Filter’, ware het niet dat een ‘Domain Filter’ het gehele domein blokkeert. Wanneer u bijvoorbeeld uw kinderen wilt beschermen voor expliciete inhoud op een bepaalde website dan kunt u naast het blokkeren van de website middels steekwoorden (zie: ‘Parental Control’) ook de gehele website blokkeren. Dit doet u middels het ‘Domain Filter’.

Acties uitvoeren op basis van tijd of datum

Met de optie ‘Schedule Rule’ configureert u wanneer een bepaalde optie actief mag zijn. Stelt u zich voor dat u uw ‘Virtual Server’ op gezette tijden toegankelijk wilt maken. Dan gebruikt u ‘Schedule Rule’ om in te stellen wanneer internetgebruikers uw Virtual Server mogen benaderen. Buiten de ingestelde periode is het vervolgens internetgebruikers niet toegestaan verbinding te maken met uw Virtual Server.

‘Schedule Rule’ is een handige optie om bepaalde toegangsblokkades te automatiseren.

Een veilige verbinding op afstand

VPN (Virtual Private Networking) stelt u in staat een beveiligde verbinding te creeeren, zodat u bijvoorbeeld thuis gebruik kunt maken van uw bedrijfsnetwerk. Een VPN verbinding is in feite niets meer dan een sterk beveiligde tunnel die, gebruikmakend van het internet, verbinding maakt met een andere computer of netwerk. Wanneer data verstuurd via een VPN wordt ontvangen door derden dan nog is de data onbruikbaar dankzij geavanceerde encryptietechnieken.

Het op afstand beheren van een netwerk

Simple Network Management Protocol (SNMP) is een beheersfunctie die u in staat stelt informatie uit de router te verzamelen. Voornoemde informatie bestaat uit informatie over het aantal op de router aangesloten computers, hun IP- en MAC-adressen en de hoeveelheid dataverkeer die op het moment van de informatieaanvraag wordt verwerkt. SNMP stelt de systeembeheerder in staat de router op afstand te beheren. Dit gebeurt veelal met speciale applicaties die het SNMP protocol ondersteunen.

Netwerktoegang toewijzen of blokkeren

Een MAC adres is een unieke code waarmee ieder netwerkproduct is uitgerust. Vaak is deze code terug te vinden op een sticker op het product. U kunt het MAC adres ook vinden door op ‘Start’, ‘Uitvoeren’ te klikken. Type ‘CMD’ en druk op enter. Type vervolgens ‘ipconfig /all’ en druk weer op enter. Bij ‘Fysiek Adres’ vindt u het MAC adres. Een MAC adres bestaat uit zes paren van ieder twee hexadecimale karakters. Bijvoorbeeld 00-0C-6E-85-03-82. MAC Address Control stelt u in staat om regels op te stellen voor MAC adressen en dus om bepaalde netwerkproducten bijvoorbeeld de toegang tot uw netwerk te ontzeggen. Wanneer u gebruik maakt van een draadloos netwerk kunt u middels MAC adres controle bijvoorbeeld instellen dat uw draadloze netwerkadapter wel verbinding mag maken met uw netwerk, maar de draadloze netwerkadapter van uw buurman niet. MAC Address Control is een mogelijkheid om uw draadloze netwerk naast WEP of WPA van een extra vorm van beveiliging te voorzien.

Uw draadloze netwerk beveiligen

WEP encryptie is een vorm van beveiliging die het draadloze signaal van uw draadloze router of modem versleuteld zodat de gegevens niet zonder meer door derden kunnen worden onderschept.

Het beveiligingsniveau wordt uitgedrukt in bits. 64-Bit WEP encryptie is het laagste beveiligingsniveau om via 128-Bit uit te komen bij het hoogste beveiligingsniveau dat WEP encryptie te bieden heeft: 256-Bit. Om WEP encryptie in te stellen dient u een hexadecimale tekenreeks of ASCII tekenreeks in te voeren. Hexadecimale tekens bestaan uit de karakters 'A' tot en met 'F' en '0' tot en met '9'. ASCII karakters omvatten alle karakters, inclusief symbolen. Wanneer u de juiste mate van beveiliging hebt gekozen en de sleutel hebt ingevoerd, dan dient u exact dezelfde sleutel ook in te voeren in alle draadloze apparaten binnen hetzelfde netwerk. Hou er rekening mee dat – wanneer u de sleutel in het eerste apparaat activeert – de verbinding met het netwerk wordt verbroken. U herstelt de verbinding door systematisch alle draadloze netwerkproducten van dezelfde sleutel te voorzien.

WPA is een vorm van beveiliging die het draadloze signaal van uw draadloze router of modem versleutelt zodat de gegevens niet zonder meer door derden kunnen worden onderschept. WPA staat voor 'Wi-Fi Protected Access' en is een zeer sterke verbetering van draadloze beveiliging. WPA maakt gebruik van een 'Pre Shared Key (PSK)'. Dit is een sleutel die van te voren in alle op het draadloze netwerk aangesloten apparaten moet worden ingesteld. Deze WPA sleutel mag niet langer zijn dan 63 (willekeurige) karakters en niet korter dan 8 (willekeurige) karakters. De beste vorm van draadloze beveiliging wordt momenteel echter gevormd door WPA2. Voornoemde standaard wordt slechts door een paar fabrikanten – waaronder Eminent – ondersteund en is daarom moeilijk te combineren met draadloze netwerkproducten van andere merken.

Wanneer u gebruik wilt maken van WPA of misschien zelfs WPA2, verzeker uzelf er dan van dat alle in uw draadloze netwerk opgenomen apparaten deze vormen van beveiliging ondersteuning. Het combineren van verschillende typen beveiliging in een draadloos netwerk is niet mogelijk en resulteren in het verlies van verbinding.

Het bereik van uw draadloze netwerk uitbreiden

WDS (Wireless Distribution System) or 'Bridging' is een optie waarmee u het bereik van uw draadloze netwerk eenvoudig kunt uitbreiden, mocht de reikwijdte van uw draadloze netwerk beperkt blijken. Via WDS gekoppelde apparaten zijn in staat uw internetverbinding te delen. U hoeft apparaten die WDS ondersteunen dus niet middels een fysieke verbinding (zoals een kabel) onderling te koppelen. In de meeste gevallen herkennen apparaten die WDS of bridging ondersteunen elkaar automatisch. Wanneer u uw netwerk middels WDS of bridging uit wilt breiden maakt u gebruik van een zogenaamde 'Range Extender'. Dit is een apparaat dat grotendeels identiek is aan een 'Access Point'. Het voordeel van het gebruik van een range extender boven een tweede draadloze router – wanneer de tweede router bridging ondersteunt – is dan een range extender aanzienlijk goedkoper is.

Index

Verklaring van Overeenstemming

Om u te verzekeren van een veilig product conform de richtlijnen opgesteld door de Europese Commissie kunt u een kopie van de Verklaring van Overeenstemming met betrekking tot uw product opvragen door een emailbericht te sturen naar: info@eminent-online.com. U kunt ook een brief sturen naar:

Eminent Computer Supplies
Postbus 276
6160 AG Geleen
Nederland

Vermeld bij uw aanvraag duidelijk 'Verklaring van Overeenstemming' en het artikelnummer van het product waarvan u de Verklaring van Overeenstemming opvraagt.

EMINENT

WWW.EMINENT-ONLINE.COM

CE

Eminent is a member of the Intronics Group