Auf Seite 17 finden Sie die Erweiterte Eminent-Bedienungsanleitung, die sich mit Netzwerkeinstellungen und Informationen über Heimnetzwerke befasst.

MANUAL

EM4450 - WLAN-Router

WWW.EMINENT-ONLINE.COM

EM4450 - WLAN-Router

Warnungen und Punkte zur Beachtung

Aufgrund von europäischen Gesetzen und Vorschriften des europäischen Parlamentes kann die Nutzung dieses Gerätes in einigen europäischen Mitgliedstaaten bestimmten Beschränkungen unterworfen sein. In bestimmten europäischen Mitgliedstaaten kann die Nutzung des Produktes sogar untersagt sein. Weitere Informationen zu diesem Thema finden Sie in der Konformitätserklärung auf der letzten Seite dieses Dokumentes.

Inhalt

Auf Seite 17 finden Sie die Erweiterte Eminent-Bedienungsanleitung, die sich mit Netzwerkeinstellungen und Informationen über Heimnetzwerke befasst.

1.0 Garantiebedingungen

Die fünfjährige Eminent-Garantie gilt für sämtliche Eminent-Produkte, sofern nicht anders erwähnt oder nicht anders beim Kauf vereinbart. Beim Kauf eines gebrauchten Eminent-Produktes gilt die restliche Garantiezeit ab Zeitpunkt des Kaufes durch den Erstkäufer. Die Eminent-Garantie gilt für sämtliche Eminent-Produkte und -Teile, die unlösbar mit dem Hauptprodukt verbunden sind.
Netzteile, Batterien/Akkus, Antennen und sämtliche sonstigen Produkte, die nicht in das Hauptprodukt integriert oder direkt damit verbunden sind sowie Produkte, deren Verschleiß zweifellos vom Verschleiß des Hauptproduktes abweicht, werden nicht durch die Eminent-Garantie abgedeckt. Die Eminent-Garantie gilt nicht, wenn Produkte falschem/unsachgemäßem Gebrauch oder externen Einflüssen ausgesetzt oder durch Personen/Institutionen geöffnet werden, die dazu nicht von Eminent autorisiert wurden.

2.0 Einleitung

Wir gratulieren Ihnen zum Kauf dieses hochwertigen Eminent-Produktes! Dieses Produkt wurde durch Eminents technische Experten eingehend geprüft. Sollte es dennoch einmal zu Problemen mit diesem Produkt kommen, genießen Sie eine fünfjährige Eminent-Garantie. Bitte bewahren Sie diese Anleitung und Ihren Kaufbeleg an einem sicheren Ort auf.

Registrieren Sie Ihr Produkt nun bei www.eminent-online.com, nutzen Sie Aktualisierungen Ihres Produktes!

2.1 Lieferumfang

Die folgenden Artikel sollten im Lieferumfang enthalten sein:

- WLAN-Router EM4450.
- Netzteil.
- UTP-Netzwerkkabel.
- CD mit Installationsassistent und Anleitungen.
- Bedienungsanleitung.

3.0 Funktionen und Merkmale

Der EM4450 ist eine optimale Lösung zum Aufbau Ihres eigenen, sicheren WLAN-Netzwerks. Der EM4450 dient dabei als WLAN-Zentrale zum Einrichten eines drahtlosen Netzwerks, auf das Sie von überall im Haus zugreifen können. Dabei arbeitet der EM4450 besonders zuverlässig und sorgt für ein stabiles und lückenlos funktionierendes WLAN-Netzwerk. Genießen Sie Ihr Netzwerk – und überlassen Sie die Arbeit Ihrem EM4450.

1. Integrierter 54 Mb/s-Zugangspunkt zum Aufbau eines drahtlosen Netzwerks.
2. Integrierter Router zur problemlosen gemeinsamen Nutzung Ihrer Internetverbindung.
3. Integrierter 4-Port-Switch für Drahtlosnetzwerke.
4. Integrierte Firewall zum Schutz Ihrer Daten.

4.0 Verbindung mit dem Router

1. Schalten Sie Ihren Computer aus.
2. Schließen Sie den EM4450 über das mitgelieferte Netzteil an eine Steckdose an.
3. Verbinden Sie das mitgelieferte UTP-Netzwerkkabel mit dem WAN-Port des EM4450.
4. Schließen Sie das andere Ende dieses UTP-Netzwerkkabels an den LAN-Port Ihres Modems an.
5. Verbinden Sie ein UTP-Netzwerkkabel mit einem der vier LAN-Ports Ihres EM4450.
6. Schließen Sie das andere Ende dieses UTP-Netzwerkkabels an den Netzwerkanschluss Ihres Computers an.

Tipp: Achten Sie darauf, dass der Router korrekt mit Strom versorgt wird, bevor Sie den EM4450 installieren. Dies können Sie leicht überprüfen, indem Sie einfach nachschauen, ob die Betriebsanzeige-LED leuchtet.
Vergewissern Sie sich auch, dass das Netzwerkkabel richtig an den EM4450 und an Ihren Computer angeschlossen ist. Um dies zu prüfen, starten Sie Ihren Computer und vergewissern sich, dass die LED des LAN-Ports leuchtet, an den Sie das UTP-Netzwerkkabel angeschlossen haben.

5.0 EM4450 mit Unterstützung der CD installieren

Wenn Sie den EM4450 an ein Kabel- oder (A)DSL-Modem anschließen, muss der EM4450 als drahtloser Router (WLAN-Router) konfiguriert werden. Am einfachsten lässt sich Ihr EM4450 mit dem Installationsassistenten konfigurieren; dies erläutern wir in diesem Kapitel. Falls Sie den Installationsassistenten, der sich auf der CD befindet, nicht benutzen möchten, können Sie den Router auch manuell konfigurieren. Siehe Kapitel 5.2.

1. Schalten Sie Ihren Computer ein, warten Sie, bis Windows komplett gestartet ist.
2. Legen Sie die mitgelieferte CD in das CD- oder DVD-Laufwerk Ihres Computers ein.
3. Ein Installationsassistent startet automatisch.
4. Folgen Sie den Anweisungen auf dem Bildschirm, bis die Installation abgeschlossen ist. Nun sollten Sie über eine funktionierende Internetverbindung verfügen.

Tipp: Falls die Installations-CD nicht automatisch starten sollte, können Sie das Installationsprogramm auch manuell starten. Führen Sie bitte die folgenden Schritte aus:

1. *Klicken Sie auf „Start“.*
2. *Klicken Sie auf „Ausführen“.*
3. *Geben Sie „x:\wizard\wizard.exe“ ein (das x steht dabei für den Laufwerkbuchstaben Ihres CD- oder DVD-Laufwerks).*
4. *Klicken Sie auf „OK“.*

6.0 Router manuell installieren

Wir befassen uns nun mit den unterschiedlichen Methoden zum Einrichten Ihres EM4450. Wenn Sie mit einem Anbieter arbeiten, der eine dieser Methoden unterstützt, müssen Sie sich lediglich an die begleitenden Hinweise halten, um schnell und sicher surfen zu können!

Einige Anbieter, die mit der DHCP-Verbindungsmethode arbeiten: @Home, Zeelandnet, Casema Wanadoo und UPC Chello.

6.1 Am EM4450 anmelden

Wenn Sie Ihren EM4450 manuell konfigurieren möchten, ist es wichtig, dass die Einstellungen Ihres Internetbrowsers und Ihre Netzwerkeinstellungen richtig konfiguriert sind. Diese Einstellungen sind gewöhnlich von Anfang an korrekt, sofern Sie keine Änderungen daran durchgeführt haben.

Tipp! Falls Sie sich hinsichtlich der Internetbrowser- und Netzwerkeinstellungen nicht sicher sein sollten, schauen Sie bitte in die Erweiterte Eminent-Bedienungsanleitung auf der CD.

Mit den folgenden Schritten können Sie sich manuell mit dem EM4450 verbinden:

1. Schalten Sie Ihren Computer ein.
2. Öffnen Sie Ihren Internetbrowser (beispielsweise Mozilla Firefox, Netscape oder auch Internet Explorer).
3. Geben Sie „http://192.168.1.1“ in die Adressleiste ein.
4. Drücken Sie die Enter-Taste.
5. Geben Sie „admin“ in das Feld „Benutzername“ ein.
6. Geben Sie „admin“ in das Feld „Kennwort “ ein.
7. Klicken Sie auf „OK“.
8. Die Begrüßungsseite wird angezeigt.

Hinweis! Um den EM4450 für Ihren Internetanbieter einrichten zu können, müssen Sie zunächst herausfinden, welche Verbindungsmethode von Ihrem Anbieter verwendet

wird – „DHCP“, „PPPoE“, „Statische IP“ oder „PPTP“. Schauen Sie sich dazu die Unterlagen Ihres Internetanbieters an oder fragen Sie ***gegebenenfalls nach.***

6.2 Konfiguration bei einer DHCP-Internetverbindung

1. Klicken Sie im linken Menü auf „Netzwerk“.
2. Klicken Sie im linken Menü auf „WAN“.
3. Wählen Sie „Dynamische IP“.
4. Geben Sie den Hostnamen (diesen erhalten Sie von Ihrem Internetanbieter) in das Feld „Hostname“ ein. Ein Beispiel: CC1234567-a (bei einer @Home-Internetverbindung).
5. Klicken Sie im linken Menü auf „MAC-Klonen“. (Dies ist nur dann erforderlich, wenn Ihr Internetanbieter mit einer MAC-Adressregistrierung arbeitet.)
6. Klicken Sie auf die „MAC klonen“-Schaltfläche.
7. Klicken Sie auf „Speichern“.
8. Schließen Sie den Internetbrowser.
9. Innerhalb von 5 Minuten sollten Sie über eine funktionierende Internetverbindung verfügen.

Tipp! Wenn Sie einen Kabel-Internetanbieter wie @Home nutzen und innerhalb von 5 Minuten keine funktionierende Internetverbindung zustande kommen sollte, lesen Sie bitte in Kapitel 11 nach.

6.3 Konfiguration bei einer Internetverbindung mit statischer IP

1. Klicken Sie im linken Menü auf „Netzwerk“.
2. Klicken Sie im linken Menü auf „WAN“.
3. Wählen Sie „Statische IP“.
4. Geben Sie die von Ihrem Internetanbieter erhaltene IP-Adresse in das Feld „IP-Adresse“ ein.
5. Geben Sie die Subnetzmaske (auch diese erhalten Sie von Ihrem Internetanbieter) in das Feld „Subnetzmaske“ ein.
6. Geben Sie die Gateway-Adresse (auch diese teilt Ihnen Ihr Internetanbieter mit) in das „Gateway“-Feld ein.
7. Geben Sie die primäre DNS-Adresse (von Ihrem Internetanbieter erhalten) in das Feld „Primärer DNS“ ein.
8. Geben Sie die sekundäre DNS-Adresse (ebenfalls von Ihrem Internetanbieter erhalten) in das Feld „Sekundärer DNS“ ein. Falls Sie keine sekundäre DNS-Adresse erhalten haben, können Sie dieses Feld leer lassen.
9. Klicken Sie auf „Speichern“.
10. Schließen Sie den Internetbrowser.
11. Innerhalb von 5 Minuten sollten Sie über eine funktionierende Internetverbindung verfügen.

6.4 Konfiguration bei einer PPPoE-Internetverbindung

1. Klicken Sie im linken Menü auf „Netzwerk“.
2. Klicken Sie im linken Menü auf „WAN“.
3. Wählen Sie „PPPoE“.
4. Geben Sie den Benutzernamen (diesen erhalten Sie von Ihrem Internetanbieter) in das Feld „Benutzername“ ein.
5. Geben Sie das Kennwort (ebenfalls von Ihrem Internetanbieter erhalten) in das Feld „Kennwort“ ein.
6. Klicken Sie auf „Speichern“.
7. Schließen Sie den Internetbrowser.
8. Innerhalb von 5 Minuten sollten Sie über eine funktionierende Internetverbindung verfügen.

6.5 Konfiguration bei einer PPTP-Internetverbindung

1. Klicken Sie im linken Menü auf „Netzwerk“.
2. Klicken Sie im linken Menü auf „WAN“.
3. Wählen Sie „PPTP“.
4. Geben Sie den Benutzernamen (diesen erhalten Sie von Ihrem Internetanbieter) in das Feld „Benutzername“ ein.
5. Geben Sie das Kennwort (ebenfalls von Ihrem Internetanbieter erhalten) in das Feld „Kennwort“ ein.
6. Geben Sie die Gateway-Adresse Ihres (A)DSL-Modems in das Feld „Server-IP-Adresse/Name“ ein.
7. Geben Sie die IP-Adresse Ihres (A)DSL-Modems in das Feld „IP-Adresse“ ein.
8. Geben Sie die Subnetzmaske Ihres (A)DSL-Modems in das Feld „Subnetzmaske“ ein.
9. Geben Sie die Gateway-Adresse Ihres (A)DSL-Modems in das Feld „Gateway“ ein.
10. Klicken Sie auf „Speichern“.
11. Schließen Sie den Internetbrowser.
12. Innerhalb von 5 Minuten sollten Sie über eine funktionierende Internetverbindung verfügen.

7.0 WLAN-Sicherheitskonfiguration

Da die Signale Ihres Drahtlosnetzwerks auch von nicht autorisierten Personen empfangen werden können, sollten Sie Ihr Netzwerk unbedingt absichern. Es gibt verschiedene Absicherungsmethoden, mit deren Hilfe Sie Ihr Netzwerk in unterschiedlichen Stufen sichern können. Bitte beachten Sie, dass eine Absicherungsmethode von sämtlichen Geräten im WLAN-Netzwerk unterstützt werden muss. Die wirkungsvollste Methode zur Absicherung drahtloser Netzwerke ist WPA (WiFi Protected Access).

Am einfachsten können Sie Ihr Netzwerk absichern, indem Sie den Installationsassistenten auf der CD nutzen; dies wird nachstehend beschrieben. Falls Sie Ihr Netzwerk nicht mit Hilfe der CD sichern möchten, können Sie diese Einstellungen alternativ auch über eine Webseite ausführen; dies wird in Kapitel 8 beschrieben.

1. Schalten Sie Ihren Computer ein, warten Sie, bis Windows komplett gestartet ist.
2. Legen Sie die mitgelieferte CD in das CD- oder DVD-Laufwerk Ihres Computers ein.
3. Ein Installationsassistent startet automatisch.
4. Wählen Sie Ihre Sprache, klicken Sie auf „Weiter“.
5. Wählen Sie „WLAN-Sicherheit konfigurieren“, klicken Sie anschließend auf „Weiter“.
6. Folgen Sie den Anweisungen auf dem Bildschirm, bis die Installation abgeschlossen ist. Ihr WLAN-Netzwerk sollte nun abgesichert sein.

Hinweis! WPA-Sicherheit wird ab Windows 2000 unterstützt. Dieses Sicherheitsverfahren kann nicht mit Windows 98 und Windows ME genutzt werden! Falls Sie also nicht mit Windows Vista, XP oder Windows 2000 arbeiten, nutzen Sie das WEP-Verfahren.

8.0 Router manuell absichern

Wenn Sie die CD nicht nutzen möchten, können Sie die Sicherheitseinstellungen auch manuell konfigurieren. In diesem Kapitel erfahren Sie, wie Sie dies bewerkstelligen. Wir empfehlen, die WPA-Verschlüsselung einzusetzen, da diese größtmögliche Sicherheit für Ihr Netzwerk bietet.

8.1 WPA-Sicherheit manuell einstellen

1. Schalten Sie Ihren Computer ein.
2. Öffnen Sie Ihren Internetbrowser (beispielsweise Mozilla Firefox, Netscape oder auch Internet Explorer).
3. Geben Sie „http://192.168.1.1“ in die Adresszeile ein. Achten Sie darauf, dass sonst nichts weiter in der Adresszeile eingetragen ist.
4. Drücken Sie die „Enter-Taste“.
5. Geben Sie „admin“ in das Feld „Benutzername“ ein.
6. Geben Sie „admin“ in das Feld „Kennwort “ ein.
7. Klicken Sie auf „OK“.
8. Die Begrüßungsseite wird angezeigt.
9. Klicken Sie im linken Menü auf „WLAN“.
10. Klicken Sie im linken Menü auf „WLAN-Einstellungen“.
11. Markieren Sie „WLAN-Sicherheit aktivieren“.
12. Wählen Sie unter „Verschlüsselungsverfahren“ das bevorzugte Sicherungsverfahren; in diesem Fall WPA-PSK/WPA2-PSK.

13. Wählen Sie WPA-PSK beim Feld „Sicherungsoption“.
14. Wählen Sie TKIP beim Feld „Verschlüsselung“.
15. Wechseln Sie nun zu „PSK-Kennwort“ (dies ist der Netzwerkschlüssel). Hier können Sie das gewünschte Kennwort eingeben. Dazu können Sie sowohl Ziffern als auch Buchstaben verwenden. Bitte denken Sie jedoch daran, dass ein WPA-Schlüssel mindestens 8 und maximal 63 Zeichen lang sein darf. Schreiben Sie sich dieses Kennwort am besten auf.
16. Klicken Sie auf „Speichern“.
17. Klicken Sie auf „OK“, klicken Sie anschließend ein weiteres Mal auf „OK“. Ihre Einstellungen werden nun gespeichert.

8.2 WEP-Sicherheit manuell einstellen

1. Schalten Sie Ihren Computer ein.
2. Öffnen Sie Ihren Internetbrowser (beispielsweise Mozilla Firefox, Netscape oder auch Internet Explorer).
3. Geben Sie „http://192.168.1.1“ in die Adresszeile ein. Achten Sie darauf, dass sonst nichts weiter in der Adresszeile eingetragen ist.
4. Drücken Sie die „Enter-Taste“.
5. Geben Sie „admin“ in das Feld „Benutzername“ ein.
6. Geben Sie „admin“ in das Feld „Kennwort “ ein.
7. Klicken Sie auf „OK“.
8. Die Begrüßungsseite wird angezeigt.
9. Klicken Sie im linken Menü auf „WLAN“.
10. Klicken Sie im linken Menü auf „WLAN-Einstellungen“.
11. Markieren Sie „WLAN-Sicherheit aktivieren“.
12. Wählen Sie unter „Verschlüsselungsverfahren“ das bevorzugte Sicherungsverfahren; in diesem Fall WEP.
13. Wählen Sie den bevorzugten Schlüsseltyp (Kennworttyp): Hier können Sie zwischen 64 Bit und 128 Bit auswählen.
14. Wenn Sie 64 Bit wählen, muss das Kennwort (der Netzwerkschlüssel) aus genau 10 Zeichen bestehen. Dies können sowohl Ziffern als auch Buchstaben sein. Wenn Sie Buchstaben verwenden, sind lediglich die Buchstaben A bis F erlaubt. Wenn Sie 128 Bit wählen, muss das Kennwort (der Netzwerkschlüssel) aus genau 26 Zeichen bestehen. Dies können ebenfalls sowohl Ziffern als auch Buchstaben sein. Wenn Sie Buchstaben verwenden, sind lediglich die Buchstaben A bis F erlaubt.
15. Diesen Schlüssel (dieses Kennwort) brauchen Sie später. Aufschreiben ist eine gute Idee.
16. Klicken Sie auf „Speichern“.
17. Klicken Sie auf „OK“, klicken Sie anschließend ein weiteres Mal auf „OK“. Ihre Einstellungen werden nun gespeichert.

Hinweis! Wir empfehlen, Sicherheitseinstellungen nur über eine Direktverbindung per Kabel zu ändern.

Hier können Sie sich Verschlüsselungsmethode, Netzwerknamen und Netzwerkschlüssel (Kennwort) notieren.

☐ *WPA* ☐ *WEP*

Netzwerkname: _____
Netzwerkschlüssel: _____

9.0 WLAN-Netzwerk am Computer konfigurieren

Nachdem Ihr Router abgesichert wurde, müssen Sie den Computer so konfigurieren, dass er das abgesicherte Netzwerk erkennen und sich damit verbinden kann.
Als Betriebssysteme werden derzeit in erster Linie Windows XP und Windows Vista eingesetzt. Daher erläutern wir die Einrichtung einer WLAN-Verbindung mit diesen beiden Betriebssystemen.

Tipp: Nachdem Sie den Router für WEP- oder WPA-Verschlüsselung konfiguriert haben, können Sie das Netzwerkkabel vom Computer trennen, bevor Sie mit Schritt 9.1 fortfahren.

9.1 Drahtloses Netzwerk unter Windows XP konfigurieren
Damit Sie eine WLAN-Verbindung unter Windows XP aufbauen können, müssen Sie die folgenden Schritte ausführen:

1. Schalten Sie Ihren Computer ein.
2. Klicken Sie auf „Start“.
3. Rufen Sie die „Systemsteuerung“ auf.
4. Wählen Sie „Netzwerkverbindungen“.
5. Ihre drahtlose Netzwerkverbindung sollte nun angezeigt werden. Klicken Sie diese Verbindung mit der rechten Maustaste an.
6. Wählen Sie „Verfügbare drahtlose Netzwerke anzeigen“. Eine Liste mit sämtlichen drahtlosen Netzwerken in Reichweite wird angezeigt.
7. Wählen Sie Ihr eigenes Netzwerk aus dieser Liste aus.
8. Wenn Sie auf „Verbinden“ klicken, teilt Ihnen Ihr Computer mit, dass das Netzwerk abgesichert und ein Netzwerkschlüssel (Kennwort) erforderlich ist.
9. Geben Sie den Netzwerkschlüssel ein, klicken Sie anschließend auf „Verbinden“.
10. Sofern Sie den richtigen Schlüssel (das richtige Kennwort) eingegeben haben, informiert Sie Windows einen Augenblick später über die Verbindung mit dem Netzwerk. Sie sind nun online.

9.2 Drahtloses Netzwerk unter Windows Vista konfigurieren

Damit Sie eine WLAN-Verbindung unter Windows Vista aufbauen können, sind die folgenden Schritte erforderlich:

1. Klicken Sie auf „Start“.
2. Rufen Sie die „Systemsteuerung“ auf.
3. Wählen Sie „Netzwerk und Internet“.
4. Rufen Sie das „Netzwerk- und Freigabecenter“ auf.
5. Klicken Sie links im Fenster auf „Netzwerkverbindungen verwalten“.
6. Klicken Sie auf „Hinzufügen“.
7. Im nächsten Bildschirm klicken Sie auf „Netzwerk hinzufügen, das sich in der Reichweite dieses Computers befindet“.
8. Im folgenden Fenster können Sie Ihr eigenes Netzwerk auswählen.
9. Klicken Sie auf „Verbinden“.
10. Ihr Computer fordert Sie nun zur Eingabe des Netzwerkschlüssels (des Kennwortes) auf. Gegen Sie Ihren Netzwerkschlüssel ein.
11. Klicken Sie auf „Verbinden“. Sofern Sie den Schlüssel richtig eingegeben haben, verbindet sich Ihr Computer mit dem Netzwerk – Sie sind online.

10.0 Internetverbindung kontrollieren

Ihr EM4450 ist mit einer erweiterten Firewall ausgestattet. Diese ermöglicht Ihnen eine nahezu vollständige Kontrolle der Internetverbindung. An der Firewall können Sie auch Einstellungen vornehmen, die bestimmten Computern eine Verbindung mit dem Internet verweigern. Auch das Blockieren von bestimmten Internetseiten ist möglich. Solche Einstellungen können Sie so einrichten, dass sie vorübergehend, permanent oder nur zu bestimmten Zeiten (z. B. zu den Bürozeiten) gelten.

10.1 Firewall einschalten

Damit Sie die Firewall konfigurieren können, müssen Sie sie zunächst einschalten. Führen Sie dazu bitte diese Schritte aus:

1. Öffnen Sie Ihren Internetbrowser (beispielsweise Mozilla Firefox, Netscape oder auch Internet Explorer).
2. Geben Sie „http://192.168.1.1“ in die Adresszeile ein. Achten Sie darauf, dass sonst nichts weiter in der Adresszeile eingetragen ist.
3. Drücken Sie die „Enter-Taste“.
4. Geben Sie „admin“ in das Feld „Benutzername“ ein.
5. Geben Sie „admin“ in das Feld „Kennwort “ ein.
6. Klicken Sie auf „OK“.
7. Die Begrüßungsseite wird angezeigt.

8. Klicken Sie auf der linken Bildschirmseite unter „Erweiterte Einstellungen“ auf „Sicherheit“.
9. Markieren Sie „Firewall einschalten“.
10. Klicken Sie auf „Speichern“.
11. Die Firewall ist nun aktiv.

10.2 Internetzugriff bestimmter IP-Adressen sperren

Über die Firewall können Sie bestimmten Computern den Zugriff auf das Internet verweigern; diese Computer werden über ihre IP-Adresse identifiziert. Wenn Sie diese Funktion nutzen möchten, müssen Sie die „IP-Adressfilterung“ einschalten. Zum Einschalten dieser Option führen Sie bitte die in Kapitel 10.1 beschriebenen Schritte aus. Bei Schritt 8 markieren Sie „IP-Adressfilterung einschalten“ und führen anschließend die Schritte 9 und 10 aus.

1. Klicken Sie auf der linken Bildschirmseite unter „Erweiterte Einstellungen“ auf „IP-Adressfilterung“.
2. Klicken Sie im nächsten Bildschirm auf „Neu hinzufügen“.
3. Geben Sie in diesem Fenster die erforderlichen Daten ein.
4. Klicken Sie auf „Gültigkeitszeit“.

In diesem Feld können Sie einen zeitlichen Rahmen vorgeben, innerhalb dessen der Internetzugriff verweigert wird. Wenn Sie den Internetzugriff beispielsweise in der Zeit von 10:00 Uhr morgens bis 8:00 Uhr abends sperren möchten, geben Sie 1000 in das Feld „Gültigkeitszeit“ und 2000 in das zweite Feld ein.

1. Geben Sie die IP-Adresse des Computers, dessen Internetzugriff Sie sperren möchten, in das Feld „LAN-IP-Adresse“ ein. Beispiel: „192.168.1.5“.
2. Wählen Sie bei „Aktion“ die Option „Sperren“.
3. Klicken Sie auf „Speichern“.
4. Nun kann der Computer, dessen IP-Adresse Sie angegeben haben, innerhalb des vorgegebenen zeitlichen Rahmens nicht mehr auf das Internet zugreifen.

Tipp: In Kapitel 11 erfahren Sie, wie Sie die IP-Adresse eines Computers abrufen können.

10.3 Internetzugriff per „Domänenfilterung“ sperren

Mit dem EM4450 können Sie den Zugriff auf bestimmte Domänen oder Webseiten sperren. Wenn Sie beispielsweise nicht möchten, dass Ihr Sohn oder Ihre Tochter sich bestimmte Seiten ansieht, können Sie einen entsprechenden Filter konfigurieren. Wenn Sie diese Funktion nutzen möchten, führen Sie bitte die in Kapitel 10.1 beschriebenen Schritte aus. Bei Schritt 8 markieren Sie allerdings „Domänenfilterung einschalten“, bevor Sie mit den Schritten 9 und 10 fortfahren.

1. Klicken Sie auf der linken Bildschirmseite auf „Domänenfilterung“.
2. Klicken Sie auf „Neu hinzufügen“.
3. Klicken Sie auf „Gültigkeitszeit“.

In diesem Feld können Sie einen zeitlichen Rahmen vorgeben, innerhalb dessen der Internetzugriff verweigert wird. Wenn Sie den Internetzugriff beispielsweise in der Zeit von 10:00 Uhr morgens bis 8:00 Uhr abends sperren möchten, geben Sie 1000 in das Feld „Gültigkeitszeit“ und 2000 in das zweite Feld ein.

4. Geben Sie die Domäne oder die Webseite, die innerhalb der definierten Zeit gesperrt werden soll, in das Feld „Domänenname“ ein. Wenn Sie beispielsweise den Zugriff auf www.google.com sperren möchten, geben Sie diese Adresse in das „Domänenname“-Feld ein.
5. Markieren Sie im „Status“-Feld die Option „Aktiv“.
6. Klicken Sie auf „Speichern“.
7. Nun kann die vordefinierte Domäne oder Webseite nicht mehr innerhalb des zeitlich vorgegebenen Rahmens aufgerufen werden.

10.4 Internetzugriff per „MAC-Adressfilterung“ sperren

Neben den oben erwähnten Verfahren zum Sperren des Internetzugriffs gibt es noch eine weitere Methode. Diese Methode ist gleichzeitig auch die effektivste. Dabei wird der Internetzugriff komplett blockiert, ohne dass Sie einen zeitlichen Rahmen vorgeben müssen. Zum Einschalten dieser Option führen Sie bitte die in Kapitel 10.1 beschriebenen Schritte aus. Bei Schritt 8 markieren Sie allerdings „MAC-Adressfilterung einschalten“, bevor Sie mit den Schritten 9 und 10 fortfahren.

1. Klicken Sie auf der linken Bildschirmseite auf „MAC-Adressfilterung“.
2. Klicken Sie auf „Neu hinzufügen“.
3. Geben Sie die zu sperrende MAC-Adresse in das Feld „MAC-Adresse“ ein.
4. In das „Beschreibung“-Feld können Sie eine kurze Erläuterung eintragen; zum Beispiel den Namen des gesperrten Benutzers.
5. Markieren Sie im „Status“-Feld die Option „Aktiv“.
6. Klicken Sie auf „Speichern“.
7. Ab jetzt wird der Internetzugriff der angegebenen MAC-Adresse komplett gesperrt.

Tipp: In Kapitel 11 erfahren Sie, wie Sie die MAC-Adresse eines Computers abrufen können.

11.0 Häufig gestellte Fragen

F: Ich erhalte die Meldung „Die IP-Adresse des Netzwerkadapters ist nicht korrekt.“. Was soll ich tun?

A: Diese Meldung erscheint, wenn der Computer keine korrekte IP-Adresse vom Router abrufen konnte. Achten Sie darauf, dass sämtliche Kabel richtig angeschlossen sind. Setzen Sie den EM4450 nötigenfalls zurück und versuchen Sie es noch einmal. Wir empfehlen, den Router über eine Kabelverbindung (nicht drahtlos) zu konfigurieren. Wenn die Kabelverbindung richtig funktioniert, können Sie die drahtlose Verbindung wie in dieser Anleitung beschrieben konfigurieren.

F: Ich habe den Router konfiguriert. Alles scheint prima zu funktionieren, allerdings kann ich nicht auf das Internet zugreifen. Mein Internetanbieter ist Chelllo.
A: Überzeugen Sie sich davon, dass Sie bei der Konfiguration die richtige MAC-Adresse angegeben haben. Bei einer falschen MAC-Adresse ist keine Internetverbindung möglich.

F: Ich habe den Router konfiguriert. Alles scheint prima zu funktionieren, allerdings kann ich nicht auf das Internet zugreifen. Mein Internetanbieter ist Chelllo / @Home / Casema oder ein anderer DHCP-Anbieter.
A: Es kommt vor, dass das Modem den Internetzugriff des Routers verweigert. Mit den folgenden Schritten sollten Sie auf das Internet zugreifen können:

1. Schalten Sie sowohl Router als auch Modem aus.
2. Warten Sie 10 Minuten.
3. Schalten Sie das Modem ein, warten Sie, bis es komplett gestartet ist. Schalten Sie nun den Router ein, warten Sie auch hier den vollständigen Start ab.
4. Die Verbindung sollte nun einwandfrei funktionieren.

F: Ich habe die obige Lösung probiert, allerdings kann ich immer noch nicht auf das Internet zugreifen. Was soll ich tun?
A: Es gibt eine weitere Möglichkeit:

1. Melden Sie sich über http://192.168.1.1 an der Webseite des Routers an.
2. Benutzername: admin. Kennwort: admin
3. Sie sind nun an der Hauptseite des EM4450 angemeldet.
4. Trennen Sie das Koaxkabel vom Modem
5. Klicken Sie auf der Router-Seite unter „WAN“ auf „Erneuern“.
6. Die IP-Adresse des Modems erscheint auf dem Bildschirm. Diese Adresse sieht meist etwa so aus: 192.168.100.x
7. Schließen Sie das Koaxkabel wieder an das Modem an, warten Sie, bis die Online/Internet-LED leuchtet.
8. Klicken Sie auf der Router-Seite auf „Erneuern“.
9. Nun sollte eine IP-Adresse, die Ihnen von Ihrem Internetanbieter zugewiesen wurde, auf dem Bildschirm erscheinen. Wenn dies so ist: Sie sind online.

F: Ich möchte meine IP-Adresse herausfinden. Wie gelange ich an diese Adresse?
A: Wenn Sie Ihre IP-Adresse erfahren möchten, führen Sie bitte die folgenden Schritte aus:

Anleitung für Windows XP/2000 und Windows Vista:

1. Klicken Sie auf „Start“.
2. Klicken Sie auf „Ausführen“.
3. Geben Sie „cmd“ ein.
4. Drücken Sie die „Enter-Taste“.
5. Geben Sie „ipconfig“ ein.
6. Drücken Sie die Enter-Taste.
7. Ihre IP-Adresse wird angezeigt.

Anleitung für Windows 98/ME:

1. Klicken Sie auf „Start“.
2. Klicken Sie auf „Ausführen“.
3. Geben Sie „winipcfg“ ein.
4. Drücken Sie die Enter-Taste.
5. Ihre IP-Adresse wird angezeigt.

F: Ich möchte die MAC-Adresse meines Netzwerkadapters herausfinden. Wie gelange ich an diese Adresse?
A: Wenn Sie die MAC-Adresse Ihres Netzwerkadapters in Erfahrung bringen möchten, führen Sie bitte die folgenden Schritte aus:

Anleitung für Windows XP/2000 und Windows Vista:

1. Klicken Sie auf „Start“.
2. Klicken Sie auf „Ausführen“.
3. Geben Sie „cmd“ ein.
4. Drücken Sie die Enter-Taste.
5. Geben Sie „ipconfig /all“ ein.
6. Drücken Sie die Enter-Taste.
7. Ihre physische Adresse wird angezeigt. Dies ist die MAC-Adresse Ihres Netzwerkadapters.

Anleitung für Windows 98/ME:

1. Klicken Sie auf „Start“.
2. Klicken Sie auf „Ausführen“.
3. Geben Sie „winipcfg“ ein.
4. Drücken Sie die Enter-Taste.
5. Die Adapter-Adresse wird angezeigt. Dies ist die MAC-Adresse Ihres Netzwerkadapters.

F: Wie setze ich den EM4450 zurück?
A: Zum Rücksetzen des EM4450 trennen Sie das Netzteil vom Router. Betätigen Sie die Rücksetztaste mit der Spitze eines Kugelschreibers oder mit einer aufgebogenen Büroklammer. Halten Sie die Rücksetztaste gedrückt, schließen Sie dabei wieder das Netzteil an den EM4450 an. Die „Sys“-LED leuchtet auf. Warten Sie, bis diese zu blinken beginnt. Lassen Sie die Rücksetztaste los. Der EM4450 wurde nun zurückgesetzt, die Werkseinstellungen wurden wieder eingestellt.

12.0 Kundendienst und Unterstützung

Diese Bedienungsanleitung wurde sorgfältig von Eminent-Experten geschrieben und ebenso sorgfältig übersetzt. Falls es dennoch einmal zu Problemen bei der Installation oder Nutzung des Produktes kommen sollte, füllen Sie bitte das Kundendienstformular unter www.eminent-online.com/support aus.

Eminent Advanced Manual

Table of contents

Why an Eminent advanced manual?

Eminent has developed the Eminent Advanced Manual especially for your ease of use. The Eminent Advanced Manual enables you to discover the advanced possibilities of your house network. The Eminent Advanced Manual will for example, help you setting up your firewall so your own network is optimally protected at all times. Of course, extensive consideration is also given to the protection of your wireless network.

The Eminent Advanced Manual is a wealth of information and a handy reference source. This will enable you to have access to functions previously only available to professional and highly advanced users.

Your tips and suggestions in the Eminent Advanced Manual?

The Eminent Advanced Manual was created in cooperation with a number of satisfied Eminent users. If you would like a certain option to be included in the Eminent Advanced Manual or you have suggestions or tips regarding the Eminent Advanced Manual, you can contact communications@eminent-online.com. Your tips and suggestions will be collected and processed in the new edition of the Eminent Advanced Manual.

Service and support

The Eminent Advanced Manual was carefully written by users and technical experts from Eminent. If you have problems installing or using the product, please contact support@eminent-online.com.

Networking settings for Windows 98 and Windows ME

1. Windows 98: Right-click 'Network neighbourhood' on your desktop.
2. Windows ME: Right-click 'My network places' on your desktop.
3. Choose 'Properties'.
4. Select 'TCP/IP'.
5. Click 'Properties'.
6. Select 'Obtain an IP Address automatically'.
7. Click the 'WINS configuration' tab.
8. Select 'Disable WINS resolution'.
9. Click the 'DNS configuration' tab.
10. Click 'Disable DNS'.
11. Click the 'Gateway' tab.
12. Remove previously installed gateways.

13. Click ‘Ok’.
14. Click ‘Ok’ in the 'Network' window.
15. Restart your computer.
16. Click 'Start'.
17. Click 'Run'.
18. Type 'Winipcfg'.
19. Click ‘Ok’.
20. Windows will show the 'IP configuration window'.
21. Select the Ethernet adapter (Networking PCI adapter) connected to the router.
22. Click 'Release all'.
23. Click 'Renew all'.
24. Click ‘Ok’.

Networking settings for Windows 2000 and Windows XP

1. Right-click 'My network places' on your desktop.
2. Choose 'Properties'.
3. Right-click 'Local area connection'.
4. Choose 'Properties'.
5. Select 'Internet protocol (TCP/IP)'.
6. Click 'Properties'.
7. Select 'Obtain an IP Address automatically'.
8. Select 'Obtain a DNS server address automatically'.
9. Click ‘Ok’.
10. Windows will show the 'Local area connection properties' window.
11. Click ‘Ok’.
12. Windows 2000: Close the 'Network and dial-up connections' window.
13. Windows XP: Close the 'Network connections' window.
14. Restart your computer.
15. Click 'Start'.
16. Click 'Run'.
17. Type 'cmd'.
18. Push enter on your keyboard.
19. Type 'ipconfig /release'.
20. Push enter on your keyboard.
21. Type 'ipconfig /renew'.
22. Push enter on your keyboard.
23. Type 'Exit'.
24. Push enter on your keyboard.

Networking settings for Windows Vista

1. Click on the Windows Vista logo (start button).
2. Choose ‘Configuration screen’.
3. Choose ‘Show network status and –tasks’.
4. Choose ‘Control network connections’.
5. Right-click on ‘LAN-connection’.
6. Choose ‘Connect.
7. If windows asks for your permission: choose ‘Continue’
8. Windows Vista now connects your LAN-connection.
9. Right-click on ‘LAN-connection’.
10. Choose ‘Properties’.
11. If windows asks for your permission: choose ‘Continue’.
12. Select ‘Internet Protocol version 4 (TCP/IPv4)’.
13. Click on ‘Properties’.
14. Choose ‘Obtain IP Address automatically.’
15. Choose ‘Obtain DNS Server address automatically’.
16. Click ‘OK’.
17. Click ‘Close’.
18. Windows Vista will now set-up your connection.

Configuring Internet Explorer 5 and 5.5

1. Start Internet Explorer.
2. Click ‘Stop’.
3. When asked to establish a connection, press ‘Cancel’.
4. Click ‘Extra’.
5. Click ‘Internet options’.
6. Click the ‘Connections’ tab.
7. Click the ‘LAN settings’ tab.
8. Uncheck ‘Find Explorer settings automatically’.
9. Uncheck ‘Use configuration script’.
10. Uncheck ‘Use proxy-server’.
11. Click ‘Ok’.
12. Remove dial-up connections by pressing ‘Delete’.
13. Click ‘Settings’ to start the ‘Internet’ Wizard.
14. Select ‘I would like to connect through a LAN network’.
15. Click ‘Next’.
16. Check ‘Automatically detect proxy-server’.
17. Click ‘Next’.
18. Click ‘No’.
19. Click ‘Next’.
20. Click ‘Complete’.
21. Close all Windows that are currently open.
22. Restart your PC.

Configuring Internet Explorer 6

1. Start Internet Explorer.
2. Click ‘Stop’.
3. When asked to establish a connection, press ‘Cancel’.
4. Click ‘Extra’.
5. Click ‘Internet options’.
6. Click the ‘Connections’ tab.
7. Click the ‘LAN settings’ tab.
8. Uncheck ‘Find Explorer settings automatically’.
9. Uncheck ‘Use configuration script’.
10. Uncheck ‘Use proxy-server’.
11. Click ‘Ok’.
12. Remove dial-up connections by pressing ‘Delete’.
13. Click ‘Settings’ to start the ‘New connection’ Wizard.
14. Click ‘Next’.
15. Select ‘Connect to the Internet’.
16. Click ‘Next’.
17. Select ‘I want to connect to the Internet manually’.
18. Click ‘Next’.
19. Select ‘Permanent broadband connection’.
20. Click ‘Next’.
21. Click ‘Complete’.
22. Close all Windows that are currently open.
23. Restart your PC.

Configuring Internet Explorer 7

1. Start internet Explorer.
2. Click ‘Stop’.
3. When asked to establish a connection, press ‘Cancel’.
4. Click ‘Extra’.
5. Click ‘Internet options’.
6. Click the ‘Connections’ tab.
7. Click the ‘LAN settings’ tab.
8. Uncheck ‘Find Explorer settings automatically’.
9. Uncheck ‘Use configuration script’.
10. Uncheck ‘Use proxy-server’
11. Click ‘Ok’.
12. Remove dial-up connections by clicking ‘Delete’.
13. Click on ‘Settings’ (at the top).
14. Choose your type of connection.
15. Windows Vista will now set-up your connection.

DHCP, Automatic allocation of IP addresses

For the development of DHCP (Dynamic Host Configuration Protocol), TCP/IP settings are configured manually on each TCP/IP client (such as your computer for example). This can be a difficult job if it is a big network or if something has to be changed regularly in the network. DHCP was developed to avoid always having to set up an IP address. With DHCP, IP addresses are allocated automatically when necessary and released when no longer required. A DHCP server has a series ('pool') of valid addresses that it can allocate to the client. When a client starts for example, it will send a message requesting an IP address. A DHCP server (there can be several in a network) responds by sending back an IP address and configuration details. The client will send a confirmation of receipt after which it can operate on the network.

Translating IP addresses and domain names

IP addresses are far from user-friendly. Domain names are however easier to remember and use. The process of translating a domain name into an address that is understandable for a machine (such as your computer) is known as 'name resolution'. A 'Domain Name System' server carries out the afore-mentioned process. Thanks to DNS, you use domain names instead of IP addresses when visiting a website or sending e-mails.

Dynamic DNS or DDNS is a DNS-related option. You can still link your IP address to a domain name using DDNS if your provider works with dynamic IP addresses ('dynamic' here means that the IP addresses change frequently). After all, the IP address to which your domain name refers will also change when your provider changes your IP address. You must register with a Dynamic DNS provider such as www.dyndns.org and www.no-ip.com in order to use Dynamic DNS.

Using a single IP address for your entire network

Network Address Translation (NAT) is an Internet standard with which a local network can use private IP addresses. Private IP addresses are those used within an own network. Private IP addresses are neither recognized nor used on the Internet. An IP address used on the Internet is also called a public IP address.

NAT enables you to share a single public IP address with several computers in your network. NAT ensures the computers in your network can use the Internet without any problems but users on the Internet will not have access to the computers in your network. You will understand that NAT also offers a certain level of security partly due to the fact that private IP addresses are not visible on the Internet.
Fortunately, most routers currently use NAT.

Security for your computer and your network

A firewall can be a software- or a hardware solution placed, as it were, between the internal network and the outside world. Firewalls generally control incoming and outgoing data. Firewalls can be adjusted to stop or allow certain information from the Internet. Firewalls can also be adjusted to stop or allow requests from outside. Rules or policies are used to adjust firewalls. These state what a firewall must stop or allow and thus form a sort of filter.

Most routers have various firewall functions. The big advantage of a firewall in a router (hardware solution) is that an attack from outside is averted before reaching your network. If you wish to use a software firewall, you could for example, use the firewall built into Windows XP Service Pack 2. There are better alternatives such as the free ZoneAlarm and the commercial packages from Norman, Norton, Panda and McAfee. These commercial packages also offer protection against viruses if required.

Making a computer available for Internet users in your network

The DMZ or DeMilitarized Zone is the zone between the outside world – the Internet – and the secure internal network. The computer placed within the DMZ is accessible via the Internet. This is in contrast to the computers that are outside the DMZ and are therefore secure. The DMZ is therefore also often used for servers that host websites. Websites must after all always be accessible via the Internet. A computer is also often placed within the DMZ if one plays a lot of online games. It is however advisable when you place a computer in the DMZ to fit a software firewall (such as the free ZoneAlarm). This is because the firewall opens all ports of the router for a computer within the DMZ. There is therefore no restriction on data transmission while this is however desirable in some situations.

Just like the DMZ function, Virtual Server enables you to make a computer, set up for example, as an FTP- or a web server, accessible from the Internet. You can state which ports in the firewall must be opened when using a Virtual Server. This is also the most important difference with the DMZ: when you place a computer in the DMZ, all ports are opened for the respective computer. If you use Virtual Server, you can open only the ports important for the respective computer.

Port Triggering or Special Apps is based on the same principle as Virtual Server. Port Triggering also enables you to make a computer within your network set up for example as an FTP- or webserver, accessible from the Internet. The ports you allocate always remain open when you use Virtual Server. With Port Triggering however, the respective ports will only be opened if requested by the respective application.

Simplifying network management

UPnP 'Universal Plug and Play': The name suggests that UpnP is very similar to the well-known – and notorious – 'Plug & Play'. Nothing is further from the truth. UPnP is completely different technology. The line of approach is that UPnP appliances must be able to communicate with one another via TCP/IP irrespective of the operating system, the programming language or the hardware. UPnP should make the user's life considerably easier.
As well as the products from a limited number of other manufacturers, most Eminent network manufacturers support UPnP. For more information on UPnP, visit: www.upnp.org.

Blocking websites with explicit content

Parental Control enables you to prevent one or more computers in your network from accessing the Internet. Parental Control often consists of several functions such as 'URL Blocking'. This function blocks websites by way of so-called 'keywords' or catchwords. Websites with explicit content are blocked in this way. URL Blocking is often combined with time and/or date blocks. Such blocks enable you to allow or block Internet access at certain times. You use 'rules' or 'policies' to set up your own schedule of blocks (see also 'Schedule Rule'). These rules describe exactly when and on what, a certain action, in this case, a block, must be applied.

Checking data traffic at package level

The package filter (or 'Packet Inspection') is a programme that checks data packages while they are passing. The intelligent package filter checks the passing dataflow or business-specific definitions such as the IP- or user address, time and date, function and a number of other definitions. The package filter can best be imagined as a gatekeeper. The 'gatekeeper' screens the passers-by: 'Who are you and where are you going?' The passers-by whom the gatekeeper considers unsafe or unreliable are kept out.

You do not have to configure the package filter in most appliances. You only have the option of activating these. The use of this option is therefore also definitely recommended.

Blocking a complete domain

A 'Domain Filter' will enable you to block an entire domain. A domain is a location on the Internet such as a website. A Domain Filter is therefore very similar to a 'URL Filter', apart from the fact that a Domain Filter blocks the entire domain. If, for example, you wish to protect your children from explicit content on a certain website, as well as blocking the website by way of catchwords (see: 'Parental Control'), you can block the entire website. You can do this using the Domain Filter.

Carrying out actions based on date or time

You can configure when a certain option may be available using the ‘Schedule Rule’ function. Imagine you wish to make your ‘Virtual Server’ available at set times. You can use the Schedule Rule to stipulate when Internet users may approach your Virtual Server. It will then not be possible for Internet users to make a connection with your Virtual Server outside the period set. Schedule Rule is a handy option for automating certain access blocks.

A safe remote connection

VPN (Virtual Private Networking) enables you to create a secure connection so you can, for example, use your business network while at home. A VPN connection is actually nothing more than a highly secure tunnel, which makes a connection with another computer or network via the Internet. Data sent via a VPN and received by third parties will still be unusable thanks to advanced encryption technology.

Remote network management

The Simple Network Management Protocol (SNMP) is a control function enabling you to collect information from the router. The above-mentioned information consists of details on the number of computers connected to the router, their IP- and MAC addresses and the amount of data traffic processed when the information is requested. SNMP enables the system administrator to control the router remotely. This is often done using special applications supporting the SNMP protocol.

Allocating or blocking network access

A MAC address is a unique code which each network product has. This code can often be found on a sticker on the product. You can also find the MAC address by clicking on ‘Start’, ‘Execute’. Type ‘CMD’ and press ‘Enter’. Then type ‘ipconfig /all’ and press ‘Enter’ again. The MAC address is shown under ‘Physical Address’. A MAC address consists of six pairs each of two hexadecimal characters. For example, 00-0C-6E-85-03-82. MAC Address Control enables you to set up rules for MAC addresses and therefore to deny for example, certain network products access to your network. When you use a wireless network, you can meanwhile use MAC Address Control to configure for example, your wireless network adapter to be able to connect to your network without the neighbouring network adapter being able to do so. MAC Address Control is a possibility, as well as WEP or WPA of providing extra security for your wireless network.

Making your wireless network secure

WEP encryption is a form of security encoding the wireless signal from your wireless router or modem so the data cannot be simply intercepted by third parties. The security level is expressed in bits. 64-Bit WEP encryption is the lowest security level

ranging up to 128-Bit for the highest level of security offered by WEP encryption: 256-Bit. You must enter a hexadecimal- or an ASCII series of characters in order to set up WEP encryption. Hexadecimal characters consist of the characters ‘A’ to ‘F’ and ‘0’ to ‘9’. ASCII characters include all characters, including symbols. When you have selected the correct level of security and entered the key, you must also enter exactly the same key into all wireless appliances within the same network. Bear in mind that – when you activate the key in the first appliance – the connection with the network will be broken. You can re-establish the network by systematically providing all wireless appliance products with the same key.

WPA is a form of security encoding the wireless signal from your wireless router or modem so the data cannot be simply intercepted by third parties. WPA stands for ‘Wi-Fi Protected Access’ and is a big improvement on wireless security. WPA uses a ‘Pre Shared Key (PSK)’. This is a key that must be put into operation on all appliances connected to the wireless network. This WPA key may not be any longer than 63 (random) characters and no shorter than 8 (random) characters. The best form of wireless protection is currently however formed by WPA2. The above-mentioned standard is only supported by a few manufacturers – including Eminent – and is therefore difficult to combine with other makes of wireless networks.

If you wish to use WPA or perhaps even WPA2, make sure that all appliances in your wireless network support this form of security. The combining of various types of security in a wireless network is not possible and will result in the loss of the connection.

Expanding the range of your wireless network

WDS (Wireless Distribution System) or ‘Bridging’ is an option with which you can easily expand the range of your wireless network should the range of your wireless network remain limited. Appliances linked via WDS can share your Internet connection. You therefore do not need to interlink appliances sharing WDS by way of a physical connection (such as a cable). Appliances supporting WDS or Bridging recognize one another automatically in most cases. You can use a so-called ‘Range Extender’ if you wish to expand your network using WDS or Bridging. This is an appliance largely similar to an ‘Access Point’. The advantage of using a Range Extender rather than a second router – if the second router bridging is supported – is that a Range Extender is considerably cheaper.

Index

Konformitätserklärung

Um Ihre Sicherheit und die Konformität des Produktes mit den Direktiven und Vorschriften der EU-Kommission sicherzustellen, können Sie eine Kopie der Konformitätserklärung für dieses Produkt anfordern, indem Sie eine E-Mail schreiben an: info@eminent-online.com. Oder schicken Sie einen Brief an:

Eminent Computer Supplies
P.O. Box 276
6160 AG Geleen
The Netherlands

Geben Sie deutlich „Declaration of Conformity" (Konformitätserklärung) und die Artikelnummer des Produktes an, für dass Sie eine Konformitätserklärung anfordern möchten.

EMINENT

WWW.EMINENT-ONLINE.COM

CE

Eminent is a member of the Intronics Group