MANUAL

EM4218 - wSURF Drahtloses ADSL2/2+-Modem

WWW.EMINENT-ONLINE.COM

EM4218 - wSURF Drahtloses ADSL2/2+-Modem

Warnungen und Punkte zur Beachtung

Entsprechend Gesetzen, Direktiven und Vorschriften des europäischen Parlaments kann der Gebrauch dieses Gerätes in bestimmten Mitgliedsstaaten der EU beschränkt sein. In bestimmten EU-Mitgliedsstaaten kann der Gebrauch dieses Produktes verboten sein. Weitere Informationen über diese Warnung finden Sie in der Konformitätserklärung auf der letzten Seite dieses Dokuments.

Inhalt

On page 12 you will find the Eminent Advanced Manual for networking settings and information about home networking. (English only)

1.0 Garantiebedingungen

Die fünfjährige Eminent-Garantie gilt für alle Eminent Produkte, außer vor oder während des Kaufs wurde eine andere Übereinkunft erwähnt. Beim Kauf eines

Eminent-Produktes aus zweiter Hand ergibt sich die verbleibende Garantiezeit aus dem Kaufdatum des ersten Besitzers. Die Eminent-Garantie gilt für alle Eminent Produkte und Teile, die unlösbar mit dem Hauptprodukt verbunden bzw. auf diesem montiert sind. Netzteile, Batterien, Akkus, Antennen und andere Produkte, die nicht im Hauptprodukt integriert sind bzw. mit diesem verbunden sind und/oder Produkte, bei denen normaler Verschleiß zweifelsfrei nach anderem Muster verläuft als bei dem Hauptprodukt, sind nicht von der Eminent-Garantie gedeckt. Produkte sind nicht von der Eminent-Garantie gedeckt, wenn diese inkorrekt/unsachgemäß verwendet, externen Einflüssen ausgesetzt oder von unbefugten Personen geöffnet wurden.

2.0 Einleitung

Glückwunsch zu Ihrem Kauf dieses hochqualitativen Eminent-Produktes! Dieses Produkt wurde von Eminents technischen Experten ausgiebig getestet. Sollten Sie mit diesem Produkt Probleme haben, sind Sie mit einer fünfjährigen Eminent-Garantie geschützt. Bitte bewahren Sie dieses Handbuch und den Kaufbeleg sicher auf.

Registrieren sie dieses Produkt jetzt auf www.eminent-online.com und erhalten Sie Produktaktualisierungen!

2.1 Funktionen und Merkmale

DerEM4218 ist ein drahtloses ADSL2/2+-Modem, das Ihnen eine stabile Internetverbindung ohne störende Kabel bietet. Der integrierte Router ermöglicht die gemeinsame Nutzung der Internetverbindung mit weiteren Computern; dazu können Sie ein Netzwerkkabel oder eine drahtlose Verbindung einsetzen.

2.2 Lieferumfang

Die folgenden Artikel sollten im Lieferumfang enthalten sein:

- EM4218 - Drahtloser ADSL2/2+-Modemrouter
- Netzteil
- Telefonkabel
- UTP-Netzwerkkabel
- CD-ROM mit Installationsassistent und Bedienungsanleitungen
- Bedienungsanleitung

2.3 Erklärung der LEDs

PWR	*Leuchtet, wenn der EM4218 eingeschaltet ist.*
WL/ACT	*Leuchtet, wenn der drahtlose Zugriffspunkt (Wireless Access Point – AP) aktiv ist.*
LAN 1, 2, 3 und 4	*Leuchten, wenn ein Computer an einen der Ports angeschlossen ist. Blinken, wenn Daten über eines der Netzwerkkabel gesendet oder empfangen werden.*
ADSL	*Fängt 30 Sekunden nach Einschalten des EM4218 an zu blinken. Leuchtet, wenn ADSL-Signal erkannt wurde (nur bei Anschluss an ein Telefonkabel mit aktivem ADSL-Signal).*
PPP	*Wenn eine PPPoE- oder PPPoA-Verbindung konfiguriert wurde, leuchtet diese LED bei funktionierender Verbindung.*

3.0 Verwendung des Installationsassistenten

Der EM4218 lässt sich am einfachsten mit dem Installationsassitenten konfigurieren; lesen Sie dazu dieses Kapitel. Wenn Sie den Assistenten (auf beiliegender CD-ROM) nicht verwenden möchten, fahren Sie mit Kapitel 4 fort.

1. Schalten Sie den Computer ein.
2. Legen Sie die CD-ROM in das CD-ROM oder DVD-Laufwerk Ihres Computers.
3. Die Software startet automatisch.
4. Befolgen Sie die Anweisungen auf ihrem Bildschirm, bis die Installation beendet ist. Jetzt sind sie mit dem Internet verbunden.

4.0 Manuelle Installation

Bei der manuellen Installation des EM4218 ist es wichtig, dass Ihr Internetbrowser und Ihr Netzwerk korrekt konfiguriert sind. Die Einstellungen sind automatisch korrekt, es sei denn, Sie haben die Einstellungen geändert. Wenn Sie bei der Einstellung ihres Internetbrowsers oder Netzwerks Fragen haben, schauen Sie bitte in die Bedienungsanleitung auf der CD-ROM.

4.1 EM4218 anschließen

1. Schalten Sie Ihren Computer aus.
2. Verbinden Sie den EM4218 über das beiliegende Netzteil mit einer Steckdose.
3. Verbinden Sie das Telefonkabel mit dem „ADSL“ Anschluss des EM4218.
4. Verbinden Sie das andere Ende des Telefonkabels mit dem ADSL-Splitter (nicht im Lieferumfang).
5. Verbinden Sie ein UTP-Netzwerkkabel mit einem der vier „LAN“ Anschlüsse Ihres EM4218.
6. Verbinden Sie das andere Ende des Netzwerkkabels mit dem Netzwerkanschluss Ihres Computers.

Ist mein EM4218 ordnungsgemäß an die Stromversorgung angeschlossen? Prüfen Sie, ob die „PWR"-LED leuchtet.

Ist das Netzwerk ordnungsgemäß verbunden? Schalten Sie den Computer ein und vergewissern Sie sich, dass die LED des LAN-Anschlusses, mit dem das UTP-Netzwerkkabel verbunden ist, leuchtet. Eine LED am Netzwerkanschluss Ihres Computers sollte ebenfalls leuchten.

4.2 EM4218 für Internetverbindung konfigurieren

Um den EM4218 für das Internet zu konfigurieren, müssen Sie zuerst eine Verbindung mit dem EM4218 herstellen. Stellen Sie eine Verbindung mit dem EM4218 her:

1. Schalten Sie Ihren Computer ein.
2. Öffnen Sie Ihren Internetbrowser (z. B. Internet Explorer, Netscape oder Firefox).
3. Geben Sie „http://192.168.1.1" in das Adressfeld ein.
4. Drücken Sie die Eingabetaste.
5. Geben Sie in das Feld „User Name" (Benutzername) „admin" ein (Hinweis: Achten Sie auf Groß- und Kleinschreibung).
6. Geben Sie in das Feld „Password" (Kennwort) „admin" ein (Hinweis: Achten Sie auf Groß- und Kleinschreibung).
7. Klicken Sie auf „Log in" (Anmelden).
8. Die Begrüßungsseite erscheint.

Tipp! Um nicht autorisierten Zugriff auf ihren EM4218 zu vermeiden, empfehlen wir Ihnen, das Kennwort zu ändern

1. *Klicken Sie auf „Tools" (Werkzeuge).*
2. *Klicken Sie auf „Password" (Kennwort).*
3. *Geben Sie „admin" in das Feld „Username" (Benutzername) ein.*
4. *Geben Sie das aktuelle Kennwort in das Feld „Old Password" (Altes Kennwort) ein.*
5. *Geben Sie das neue Kennwort in das Feld „New Password" (Neues Kennwort) ein.*
6. *Geben Sie das neue Kennwort erneut im Feld „Confirmed Password" (Kennwort bestätigen) ein.*
7. *Klicken Sie auf „Submit" (Übertragen).*
8. *Klicken Sie auf „OK".*

Schreiben Sie das neue Kennwort auf, damit Sie sich auch später erneut anmelden und die Einstellungen ändern können.

Benutzername: admin
Kennwort: _____

4.3 Konfiguration für PPP-Anbieter

1. Klicken Sie auf „Setup Wizard“ (Einrichtungsassistent).
2. Wählen Sie Ihr Land im Feld „Country“ (Land) aus; beispielsweise „Deutschland“.
3. Wählen Sie Ihren Internetanbieter im Feld „ISP“ aus.
4. Klicken Sie auf „Next“ (Weiter).
5. Geben Sie Ihren (A)DSL-benutzernamen in das Feld „Username“ (Benutzername) ein.
6. Geben Sie Ihr Kennwort in das Feld „Input Password“ (Kennwort eingeben) ein.
7. Geben Sie das Kennwort noch einmal im Feld „Confirm Password“ (Kennwort bestätigen) ein.
8. Klicken Sie auf „Save“ (Speichern) – die Einstellungen werden gespeichert, der EM4218 startet neu.

4.4 Konfiguration für DHCP-Anbieter

1. Klicken Sie auf „Setup Wizard“ (Einrichtungsassistent).
2. Wählen Sie Ihr Land im Feld „Country“ (Land) aus; beispielsweise „Deutschland“.
3. Wählen Sie Ihren Internetanbieter im Feld „ISP“ aus.
4. Wählen Sie „DHCP (Get IP dynamically from ISP)“ (IP dynamisch vom Anbieter beziehen) in das Feld „Connection Type“ (Verbindungstyp) ein.
5. Klicken Sie auf „Next“ (Weiter).
6. Klicken Sie auf „Save“ (Speichern) – die Einstellungen werden gespeichert, der EM4218 startet neu.

4.5 Konfiguration für sonstige Anbieter

Falls Ihr Anbieter nicht in der Liste des Assistenten aufgeführt wird, können Sie Ihren Anbieter nach den richtigen Einstellungen fragen. Auf folgende Weise geben Sie diese Einstellungen in den EM4218 ein:

1. Klicken Sie auf „Advanced“ (Erweitert).
2. Klicken Sie auf „WAN“.
3. Geben Sie die vom Anbieter erhaltenen Einstellungen ein.
4. Klicken Sie auf „Add“ (Hinzufügen).
5. Klicken Sie auf „Save“ (Speichern – rechts oben).
6. Klicken Sie auf „OK“ – der EM4218 startet neu.

5.0 Drahtloses Netzwerk absichern

Um zu vermeiden, dass ungebetene Gäste Ihr drahtloses Netzwerk verwenden, sollten Sie Ihr Drahtlosnetzwerk absichern. Sie können Ihr drahtloses Netzwerk auf verschiedene Weise absichern. Um eine Methode in ihrem Netzwerk verwenden zu können, müssen alle Drahtlosgeräte diese Methode unterstützen. Wir empfehlen die sicherste Schutzvariante: WPA2 (WiFi Protected Access).

1. Öffnen Sie Ihren Internetbrowser (z. B. Internet Explorer, Netscape oder Firefox).
2. Geben Sie „http://192.168.1.1" in das Adressfeld ein.
3. Drücken Sie die Eingabetaste.
4. Geben Sie in das Feld „User Name" (Benutzername) „admin" ein (Hinweis: Achten Sie auf Groß- und Kleinschreibung).
5. Geben Sie in das Feld „Password" (Kennwort) „admin" ein (Hinweis: Achten Sie auf Groß- und Kleinschreibung).
6. Klicken Sie auf „Advanced" (Erweitert).
7. Klicken Sie auf „Wireless" (Drahtlos).
8. Klicken Sie auf „Security" (Sicherheit).
9. Bei WPA-Absicherung (empfohlen) fahren Sie mit Kapitel 5.1, bei WEP-Absicherung mit Kapitel 5.2 fort.

WPA2-Absicherung wird von Windows 2000 und neueren Windows-Versionen unterstützt. Wenn eine ältere Windows-Version nutzen, fahren Sie mit Kapitel 5.2 fort.

5.1 WPA2-Absicherung (empfohlen)

1. Wählen Sie im Feld „Encryption" (Verschlüsselung) den Eintrag „WPA2 (AES)".
2. Wählen Sie „Personal (Pre-Shared Key)" (Persönlich (zuvor ausgehandelter Schlüssel)) im Feld „WPA Authentication Mode" (WPA-Authentisierungsmodus) .
3. Wählen Sie „Passphrase" (Kennwort) im Feld „Pre-Shared Key Format" (zuvor ausgehandeltes Schlüsselformat).
4. Geben Sie das Kennwort in das Feld „Pre-Shared Key" (zuvor ausgehandelter Schlüssel) ein. Z. B. „IhrName01". Verwenden Sie keine Sonderzeichen, achten Sie darauf, dass das Kennwort mindestens 8 Zeichen lang ist!
5. Schreiben Sie das Kennwort auf. *
6. Klicken Sie auf „Submit" (Übertragen).
7. Klicken Sie auf „Save" (Speichern – rechts oben).

5.2 WEP-Absicherung

1. Wählen Sie im Feld „Encryption" (Verschlüsselung) den Eintrag „WEP".
2. Klicken Sie auf „Set WEP Key" (WEP-Schlüssel festlegen).
3. Ein neuer Bildschirm öffnet sich.
4. Wählen Sie im Feld „Key Length" (Schlüssellänge) entweder 64 oder 128 Bit.
5. Wählen Sie im Feld „Key Format" (Schlüsselformat) entweder „ASCII" oder „Hex" aus.
6. Wählen Sie „Key 1" (Schlüssel 1) im Feld „Default Tx Key" (Standard-Übertragungsschlüssel).
7. Geben Sie ein Kennwort in das Feld „Encryption Key 1" (Schlüssel 1) ein. Nutzen Sie keine Sonderzeichen, achten Sie darauf, dass das Kennwort exakt 5, 10, 13 oder 26 Zeichen lang ist – abhängig von den weiteren Schlüsseleinstellungen.
8. Schreiben Sie das Kennwort auf. *
9. Klicken Sie auf „Submit" (Übertragen).
10. Klicken Sie auf „Save" (Speichern – rechts oben).

Wurde die Sicherheitsfunktion (WPA2 oder WEP) bereits am EM4218, jedoch noch nicht am Drahtlosnetzwerkadapter aktiviert, so wird die Verbindung unterbrochen. Sobald die Sicherheitseinstellungen auch am Drahtlosnetzwerkadapter vorgenommen wurden, wird die Verbindung wieder hergestellt.

** Schreiben Sie verwendete Sicherheitsmethode und Kennwort auf:*
☐ *WPA2* ☐ *WEP*

Kennwort : _____

6.0 Internetverbindung steuern

Zur Verbesserung der Netzwerksicherheit können Sie die MAC-Adressenkontrolle Ihres EM4218 aktivieren. Eine MAC-Adresse ist ein eindeutiger Code, der jedem Netzwerkgerät zugewiesen wurde. Über die MAC-Adressenkontrolle können Sie speziellen Netzwerkgeräten den Zugriff auf das Netzwerk erlauben. Sämtliche anderen Geräte werden abgewiesen. Wenn Sie nur ihre eigene MAC-Adresse hinzufügen, können nur Sie sich mit Ihrem Netzwerk verbinden.

Oft ist die MAC-Adresse auf einem Aufkleber am Netzwerkgerät zu finden. Sie können sie auch über folgende Schritte herausfinden:

1. *Klicken Sie auf „Start“*
2. *Klicken Sie auf „Ausführen“.*
3. *Geben Sie „CMD“ ein.*
4. *Drücken Sie die Eingabetaste.*
5. *Geben Sie „ipconfig /all” ein.*
6. *Drücken Sie die Eingabetaste.*
7. *Die „Physikalische Adresse“ ist die MAC-Adresse.*

Tipp! Zu Ihrer Sicherheit ist die Firewall per Vorgabe eingeschaltet. Wir empfehlen Ihnen auch die Installation eines Virenscanners und dessen regelmäßige Aktualisierung.

6.1 MAC-Adressenkontrolle, Benutzer blockieren

1. Öffnen Sie Ihren Internetbrowser (z. B. Internet Explorer, Netscape oder Firefox).
2. Geben Sie „http://192.168.1.1” in das Adressfeld ein.
3. Drücken Sie die Eingabetaste.
4. Geben Sie in das Feld „User Name“ (Benutzername) „admin“ ein (Hinweis: Achten Sie auf Groß- und Kleinschreibung).
5. Geben Sie in das Feld „Password“ (Kennwort) „admin“ ein (Hinweis: Achten Sie auf Groß- und Kleinschreibung).
6. Klicken Sie auf „Advanced“ (Erweitert).
7. Klicken Sie auf „Wireless“ (Drahtlos).

8. Klicken Sie auf das Register „Access Control“ (Zugriffssteuerung).
9. Wählen Sie „Allow Listed“ (Gelistete zulassen).
10. Geben Sie die MAC-Adresse des Netzwerkgerätes ein, dem Sie den Zugang zu Ihrem Netzwerk gestatten möchten.
11. Klicken Sie auf „Submit“ (Übertragen).
12. Wiederholen Sie die Schritte 11 und 12, falls Sie weitere Netzwerkgeräte zu Ihrem Netzwerk hinzufügen möchten.
13. Klicken Sie auf „Save“ (Speichern – rechts oben).
14. Nun können sich nur die von ihnen explizit angegebenen Netzwerkgeräte mit Ihrem Netzwerk verbinden.

7.0 WDS, Netzwerkreichweite erweitern

Mit der WDS-Funktion können Sie die Reichweite ihres Drahtlosnetzwerks erweitern und dem gesamten Netzwerk die Verbindung mit dem Internet ermöglichen. Über WDS können Sie durch Installation mehrerer Router, die über WDS als Repeater arbeiten, die Netzwerkreichweite erweitern. Diese Konfiguration benötigt nur eine Internetverbindung. Alle Router, die über WDS verbunden sind, haben Zugang zum Internet. D. h., Sie müssen die LAN- oder WAN-Anschlüsse der Router nicht über Kabel anbinden. Mit WDS können Sie eine Internetverbindung drahtlos mit anderen Drahtlosroutern oder Zugriffspunkten, die ebenfalls WDS unterstützen, teilen.

7.1 WDS-Funktion des EM4218 aktivieren

So verwenden Sie die WDS-Funktion. In diesem Beispiel werden zwei Drahtlosrouter verwendet. Der EM4218 ist mit dem Internet verbunden. Der andere Drahtlosrouter leitet die Funksignale weiter (Repeater-Funktion).

1. Schalten Sie Ihren Computer ein.
2. Öffnen Sie Ihren Internetbrowser (z. B. Internet Explorer, Netscape oder Firefox).
3. Geben Sie „http://192.168.1.1” in das Adressfeld ein.
4. Drücken Sie die Eingabetaste.
5. Geben Sie in das Feld „User Name“ (Benutzername) „admin“ ein (Hinweis: Achten Sie auf Groß- und Kleinschreibung).
6. Geben Sie in das Feld „Password“ (Kennwort) „admin“ ein (Hinweis: Achten Sie auf Groß- und Kleinschreibung).
7. Klicken Sie auf „Log in“ (Anmelden).
8. Der Router zeigt einen Begrüßungsbildschirm an.
9. Klicken Sie auf „Advanced“ (Erweitert).
10. Klicken Sie auf „Wireless“ (Drahtlos).
11. Klicken Sie auf „Setting“ (Einstellungen).
12. Stellen Sie „Mode“ (Modus) auf WDS ein.
13. Klicken Sie auf „Submit“ (Übertragen).
14. Klicken Sie auf „OK“.
15. Klicken Sie im oberen Menü auf „WDS“.
16. Markieren Sie „Enable WDS“ (WDS aktivieren).

17. Geben Sie die WLAN-MAC-Adresse (BSSID) des anderen Routers in das Feld „Add WDS AP“ (WDS-AP hinzufügen) ein. Die MAC-Adresse finden Sie meist an der Unterseite des Routers.
18. Falls die Adresse nicht auffindbar ist, klicken Sie auf die Schaltfläche „Show AP“ (Zugriffspunkt anzeigen). Notieren Sie sich die BSSID des Routers, den Sie über WDS anbinden möchten, schließen Sie dann den „Show AP“-Bildschirm.
19. Klicken Sie auf „Submit“ (Übertragen).
20. Wenn Sie weitere Router zu Ihrem WDS-Netzwerk hinzufügen möchte, wiederholen Sie die Schritte 17 und 18 mit jedem weiteren Router.
21. Klicken Sie auf „Save“ (Speichern).
22. Klicken Sie auf „OK“.

Um eine WDS-Verbindung herzustellen, müssen Sie die MAC-Adresse des EM4218 in das empfangende Gerät eingeben. Weitere Informationen finden Sie in der Bedienungsanleitung des empfangenden Gerätes.

Sofern Ihr Drahtlosnetzwerk abgesichert ist, müssen Sie die Sicherheitseinstellungen auch bei Ihren anderen Drahtlosgeräten entsprechend konfigurieren. Im WDS-Modus kann lediglich mit WEP gesichert werden. Schauen Sie sich bitte Kapitel 5.2 zur WEP-Absicherung an.

7.2 Was Sie bei Verwendung von WDS beachten sollten

- Alle Router, die über WDS verbunden sind, müssen im selben IP-Bereich liegen (z. B. 192.168.1.1 für Router A, 192.168.1.200 für Router B). Es kann vorkommen, dass Sie für das Empfangsgerät eine feste IP-Adresse einstellen müssen.
- Die WEP-Sicherheitseinstellungen müssen bei beiden Geräten identisch sein.
- Die Kanäle für drahtlose Verbindungen müssen identisch sein.
- Die Namen (SSIDs) für drahtlose Verbindungen müssen nicht identisch sein.
- Wir empfehlen, die MAC-Adressenkontrolle zusammen mit WDS zu verwenden.
- DHCP-Server am zweiten (oder dritten, vierten) Router müssen deaktiviert werden.

Achtung! WPA2 kann in diesem Fall nicht zur Verbindungsabsicherung verwendet werden.

8.0 Häufig gestellte Fragen

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

A: Diese Meldung wird angezeigt, wenn der Computer keine korrekte IP-Adresse vom Router beziehen konnte. Überzeugen Sie sich davon, dass sämtliche Kabel richtig angeschlossen sind. Setzen Sie den EM4218 nötigenfalls zurück und versuchen Sie es noch einmal. Wir empfehlen, der Router über eine

Kabelverbindung (nicht drahtlos) zu konfigurieren. Wenn die Kabelverbindung richtig arbeitet, knen Sie die Drahtlosverbindung wie in dieser Anleitung beschrieben einrichten.

F. Wie setze ich den EM4218 zurück?

A: Sie können das Gerät mit dem folgenden Schritten zurücksetzen:

1. Schalten Sie das Gerät ein, warten Sie, bis es komplett gestartet ist.
2. Halten Sie die Rücksetztaste („Reset“) neben der Ein-/Austaste etwa 20 Sekunden lang gedrückt; dazu können Sie eine aufgebogene Büroklammer verwenden.
3. Das Gerät wurde zurückgesetzt.

F: Das Drahtlossignal ist schwach oder instabil . Woran kann das liegen?

A: Stellen Sie das Gerät an einer anderen Stelle auf; achten Sie darauf, ob die Signalstärke zunimmt. Stellen Sie das Gerät an einer möglichst freien Stelle auf. Ein Schaltkasten ist beispielsweise ein denkbar ungünstiger Ort für ein Drahtlosgerät.

A: Sie können den Funkkanal des Gerätes ändern und schauen, ob die Signalstärke zunimmt. Führen Sie dazu die folgenden Schritte aus:

1. Öffnen Sie Ihren Internetbrowser (z. B. Internet Explorer, Netscape oder Firefox).
2. Geben Sie „http://192.168.1.1” in das Adressfeld ein.
3. Drücken Sie die Eingabetaste.
1. Geben Sie in das Feld „User Name“ (Benutzername) „admin“ ein (Hinweis: Achten Sie auf Groß- und Kleinschreibung).
2. Geben Sie in das Feld „Password“ (Kennwort) „admin“ ein (Hinweis: Achten Sie auf Groß- und Kleinschreibung).
4. Klicken Sie auf „Advanced“ (Erweitert).
5. Klicken Sie auf „Wireless“ (Drahtlos).
6. Stellen Sie bei „Channel“ (Kanal) eine andere Zahl ein; z. B. 3.
7. Klicken Sie auf „Submit“ (Übertragen).
8. Klicken Sie auf „Save“ (Speichern).
9. Klicken Sie auf „OK“.

9.0 Service und Kundendienst

Dieses Benutzerhandbuch wurde von Eminents technischen Experten sorgfältig geschrieben. Wenn Sie Probleme bei der Installation oder mit der Bedienung eines Produktes haben, einfach den Support-Vordruck ausfüllen unter: www.eminent-online.com/support.

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 (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.

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

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-adresses 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