

Anleitung zur Einrichtung der Drahtlosverbindung (WLAN)

Um Ihre Drahtlosverbindung (WLAN) abzusichern müssen Sie die Verschlüsselung im Accesspoint konfigurieren.

Ein ungesichertes WLAN kann dazu führen, dass unbefugte Personen auf alle Ihre im Netzwerk befindlichen Geräte zugreifen, Ihre Daten stehlen, sie manipulieren, oder Ihren Internetzugang nutzen. Wenn unbefugte Ihren Internetzugang für illegale Zwecke nutzen, z.B. das Herunterladen von urheberrechtlich geschützten Dateien, kann das sogar rechtliche Konsequenzen für Sie haben.

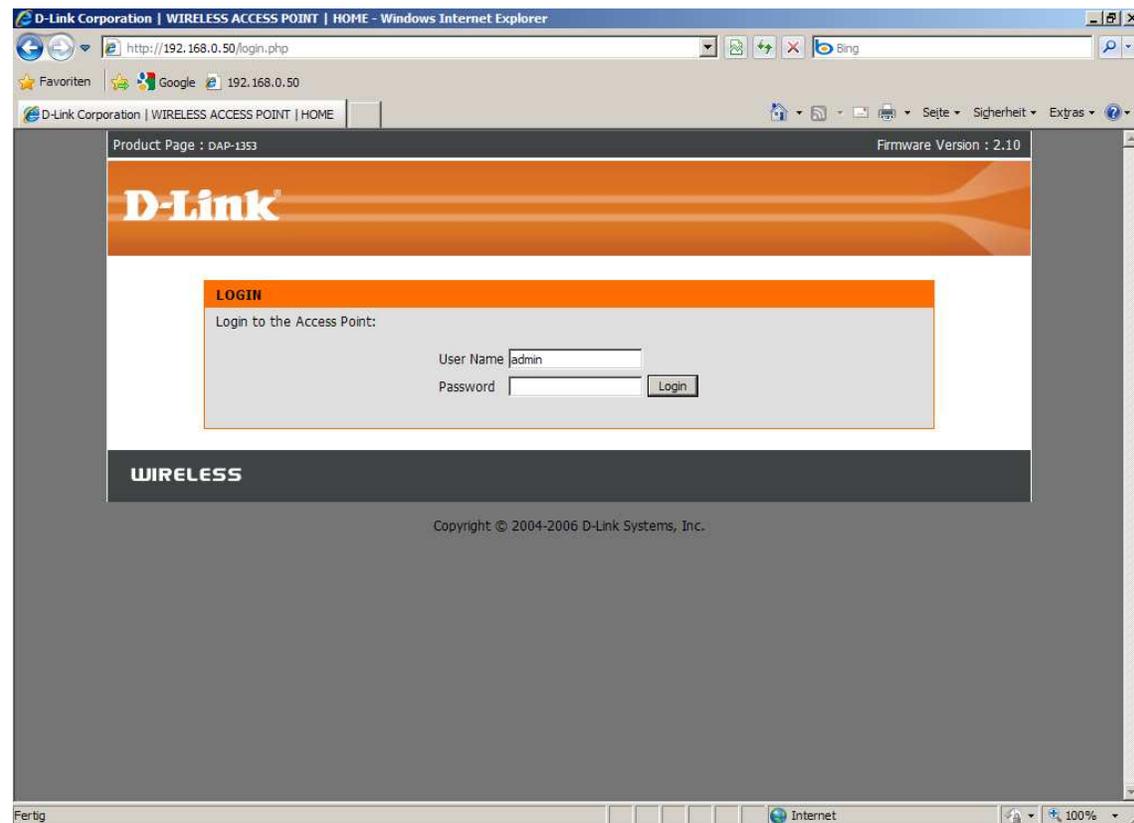
Daher ist es sehr zu empfehlen das WLAN abzusichern.

1. Greifen Sie per Webbrowser auf die Konfiguration des Accesspoints zu.

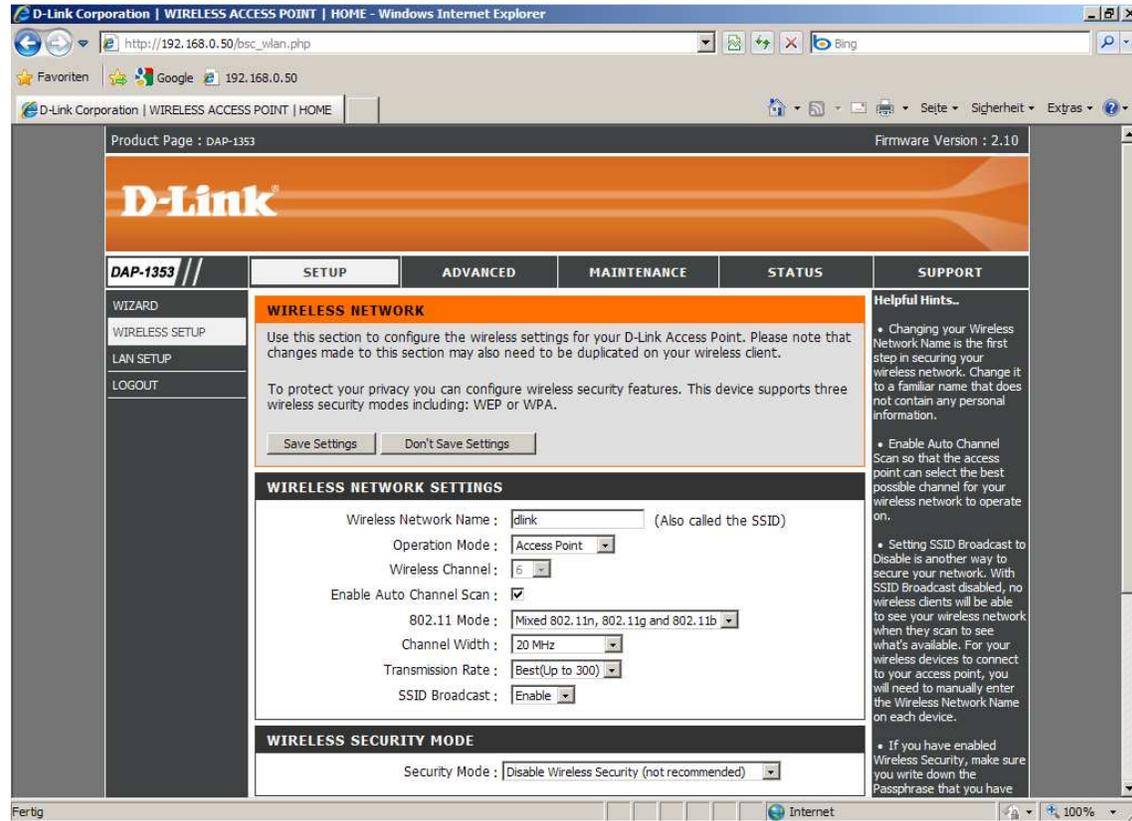
Die Standard Adresse ist <http://192.168.0.50>

2. Im Auslieferungszustand ist auf die Konfiguration kein Passwort gesetzt.

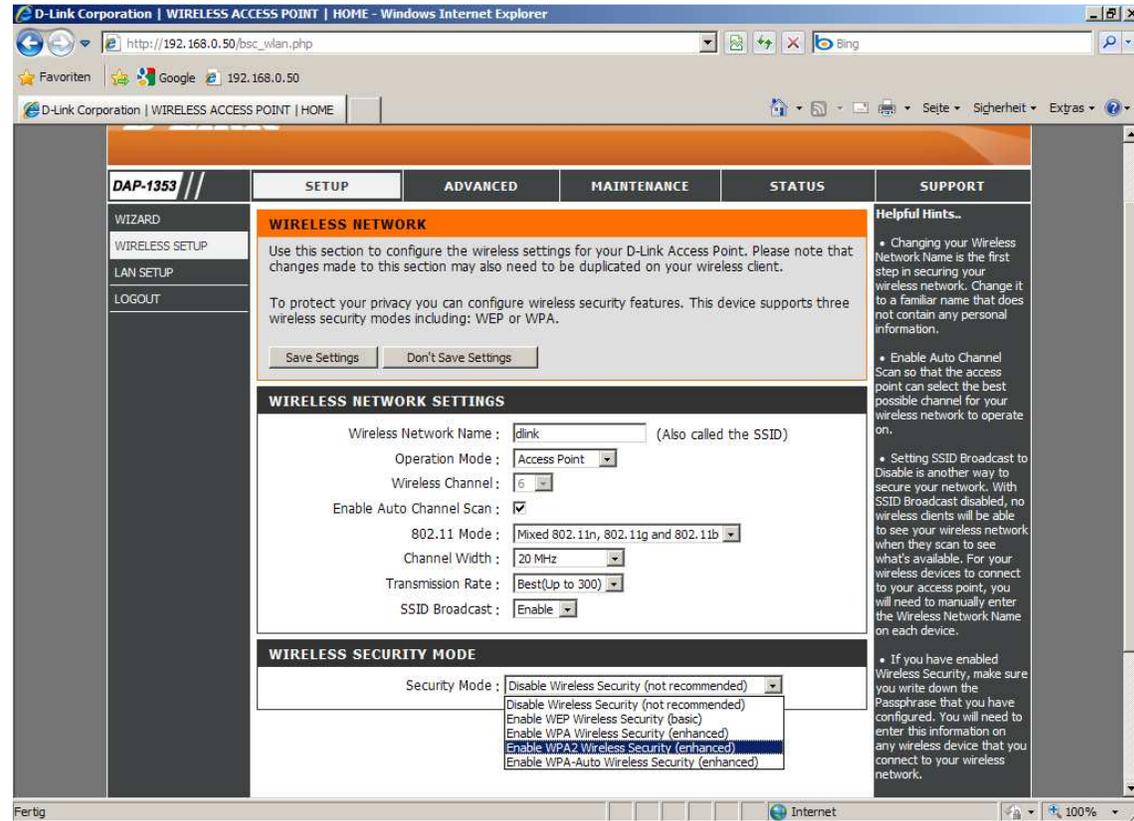
Als „User Name“ wählen Sie „admin“ aus, lassen das „Kennwort“ Feld leer und klicken Sie auf „Login“.



3. Wählen Sie oben das Menü „Setup“ und links „Wireless Setup“ aus.



4. Vergeben Sie bei „Wireless Network Name“ Ihrem WLAN einen Namen. Dies ist die SSID. Der Name sollte nicht auf Sie oder einen Gerätetyp hindeuten.



5. Sie können „Enable Auto Channel Scan“ aktivieren, damit der Accesspoint selbst einen möglichst freien Kanal auswählt, oder Sie können einen „Wireless Channel“ selbst auswählen.
6. Über „SSID Broadcast“ können Sie die SSID verstecken. Dies sollten Sie zunächst auf „enable“ belassen, da manche WLAN Adapter andernfalls nicht einwandfrei arbeiten können. Eine zusätzliche Sicherheit bringt eine versteckte SSID zudem kaum.
7. Wählen Sie bei „Security Mode“ die Art der Verschlüsselung aus.

Disable Wireless Security = Ihr WLAN ist unverschlüsselt

Enable WEP Wireless Security = Ihr WLAN wird mit WEP verschlüsselt. Dies ist eine mittlerweile sehr unsichere Verschlüsselung.

Enable WPA –Wireless Security = Um eine WPA-PSK Konfiguration vorzunehmen.

Enable WPA2 Wireless Security = (empfohlen) Um eine WPA2-PSK Konfiguration vorzunehmen.

Enable WPA2-Auto Wireless Security = WLAN Clients können sich mit WPA-PSK TKIP oder WPA2- PSK AES auf Ihr WLAN verbinden.

8. Haben Sie WEP ausgewählt können Sie nun die Schlüssellänge auswählen und den Schlüssel eingeben. Klicken Sie dann auf „Save Settings“.

Eine WEP-Verschlüsselung zu nutzen empfehlen wir nicht.

9. WPA-PSK / WPA2-PSK konfigurieren.

Bei „Security Mode“ haben Sie die Wahl zwischen:

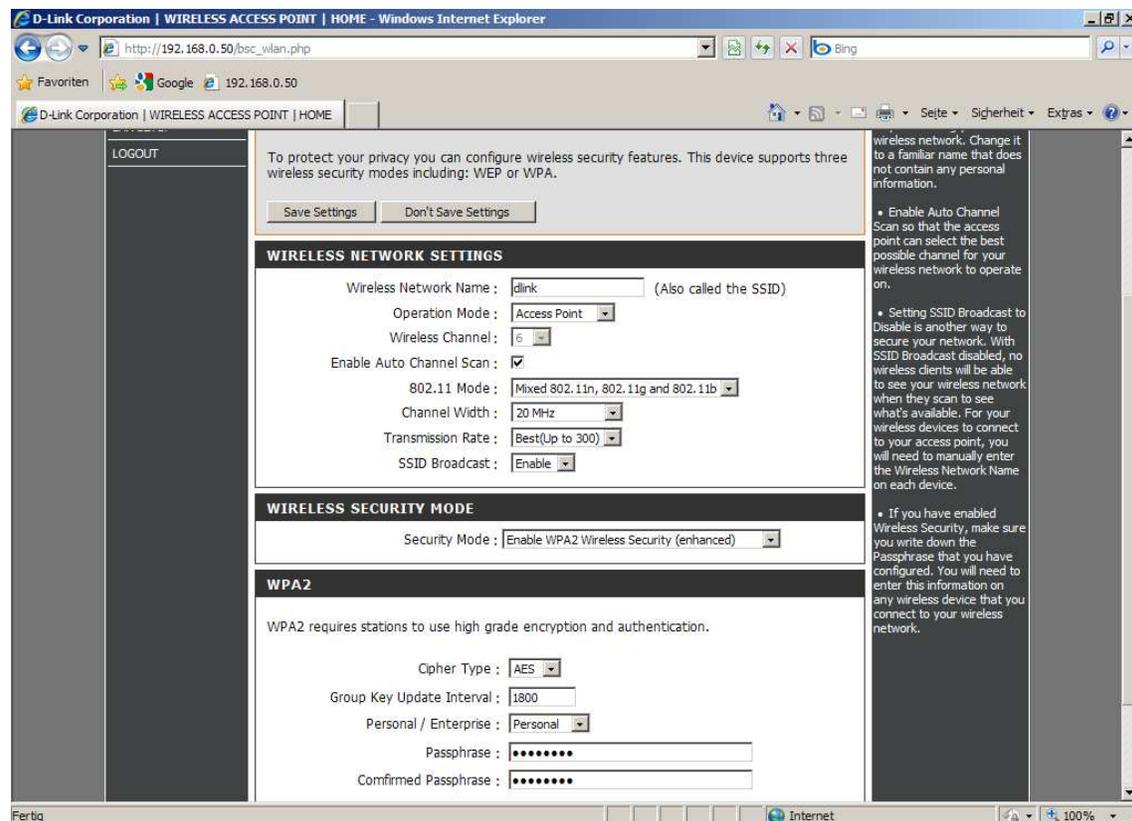
Disable Wireless Security = Ihr WLAN ist unverschlüsselt

Enable WEP Wireless Security = Ihr WLAN wird mit WEP verschlüsselt. Dies ist eine mittlerweile sehr unsichere Verschlüsselung.

Enable WPA –Wireless Security = Um eine WPA-PSK Konfiguration vorzunehmen.

Enable WPA2 Wireless Security = (empfohlen) Um eine WPA2-PSK Konfiguration vorzunehmen.

Enable WPA2-Auto Wireless Security = WLAN Clients können sich mit WPA-PSK TKIP oder WPA2- PSK AES auf Ihr WLAN verbinden.



10. Wählen Sie den Verschlüsselungstyp (Cipher Type) aus. (empfohlen: „AES“)

Wenn vorher Enable WPA –Wireless Security gewählt wurde wählen Sie TKIP aus.

Wenn vorher **Enable WPA2 Wireless Security** gewählt wurde wählen Sie **AES** aus.
(empfohlen)

Wenn vorher **Enable WPA2-Auto Wireless Security** ausgewählt wurde (nicht empfohlen)
wählen Sie **TKIP** und **AES** aus.

11. Geben Sie bei „Passphrase“ und „Confirm Passphrase“ denselben mindestens 8 und höchstens 63 Zeichen langen, nicht zu erratenden Schlüssel ein.

Verwenden Sie dabei primär Zeichen von A-Z (groß oder klein) und Zahlen von 0-9. Sonderzeichen können mitunter zu Problemen führen da dies beide Seiten beherrschen müssen.

Merken Sie sich den eingegebenen Schlüssel, da dieser in den WLAN Client eingetragen werden muss.

12. Schieben Sie das Konfigurationsfenster wieder ganz nach oben.

Klicken Sie auf „Save Settings“.

Die Einstellungen werden nun vom Accesspoint gespeichert und übernommen.

Product Page : DAP-1353 Firmware Version : 2.10

D-Link

DAP-1353 // SETUP ADVANCED MAINTENANCE STATUS SUPPORT

WIRELESS NETWORK

Use this section to configure the wireless settings for your D-Link Access Point. Please note that changes made to this section may also need to be duplicated on your wireless client.

To protect your privacy you can configure wireless security features. This device supports three wireless security modes including: WEP or WPA.

Save Settings Don't Save Settings

WIRELESS NETWORK SETTINGS

Wireless Network Name : WLAN (Also called the SSID)

Operation Mode : Access Point

Wireless Channel : 6

Enable Auto Channel Scan :

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Channel Width : 20 MHz

Transmission Rate : Best(Up to 300)

SSID Broadcast : Enable

WIRELESS SECURITY MODE

Security Mode : Disable Wireless Security (not recommended)

Helpful Hints.

- Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.
- Enable Auto Channel Scan so that the access point can select the best possible channel for your wireless network to operate on.
- Setting SSID Broadcast to Disable is another way to secure your network. With SSID Broadcast disabled, no wireless clients will be able to see your wireless network when they scan to see what's available. For your wireless devices to connect to your access point, you will need to manually enter the Wireless Network Name on each device.
- If you have enabled Wireless Security, make sure you write down the Passphrase that you have

Troubleshooting:

Problem: Der WLAN Client (PC/Laptop) verbindet sich nicht auf den Accesspoint:

- a.)
Viele Verbindungsprobleme beruhen auf alten Treibern. Stellen Sie daher bitte sicher, dass der WLAN Client die aktuellen Treiber des Herstellers installiert hat.
- b.)
Überprüfen Sie die Richtigkeit der Verschlüsselung und des eingegebenen Schlüssels.
- c.)
Stellen Sie bitte sicher, dass sich der WLAN Client auf Ihr eigenes WLAN verbindet und nicht zufällig auf das eines Nachbarn. Zur eindeutigen Identifizierung Ihres WLAN vergeben Sie Ihrem eine eigenständige SSID.
- d) Vermeiden Sie die WPA-AUTO Option sondern wählen Sie die exakte Verschlüsselung zum Beispiel WPA2-PSK AES manuell aus.

Problem: Schlechter Empfang oder schlechter Datendurchsatz:

- a.)
Ändern Sie im Accesspoint den Kanal. Jeder Kanal ist eine andere Frequenz, wodurch Störern aus dem Weg gegangen werden kann.
- b.)
Positionieren Sie den Accesspoint und den Client möglichst anders. Eine schlechte Position ist direkt an einer Wand, in einem Schrank, im Keller oder ähnliches.
- c.)
Richten Sie die Antennen aus. Soll das Funksignal primär zu den Seiten laufen, richten Sie die Antennen senkrecht in W-Form aus (\ | /).
Soll das Funksignal primär nach oben oder unten laufen, richten Sie die Antennen waagrecht in W-Form aus (\ | /).

Weitere Informationen können Sie unserem Wireless Howto entnehmen das Sie unter ftp://ftp.dlink.de/anleitungen/HowTo/D-Link_Wireless_HOWTO.pdf herunterladen können.

