

Yetkisiz Kablosuz İstemcileri Engelleme

Yetkisiz Wi-Fi istemcilerinin AP veya Wi-Fi Router'inize bağlanmasını önlemek ve local networkünüzü güvende tutmak için birkaç ipucu.

Güvenliği etkinleştirin ve WPA2'yi kullanın

Kolaylık sağlamak için güvenliği devre dışı bırakmayın. Ve yeterince uzun bir şifre kullanmak güvenliğiniz için daha iyi bir sonuç verir. Bu arada, WPA2 şu anda uyguladığımız en güvenli protokol ve önerdiğimiz güvenlik yöntemidir.

Wireless LAN >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
Mode:			WPA2/PSK
WPA			
Encryption Mode:			TKIP for WPA/AES for WPA2
Pre-Shared Key(PSK):			*****
Type 8~63 ASCII character or 64 Hexadecimal digits leading by "0x", for example "cfs01a2..." or "0x655abcd....".			

SSID'yi değiştirin ve gizleyin

Router'in Wireless networkün varlığını yayınlamaması için **Wireless LAN >> General Setup**'da, Hide SSID etkinleştirin. Ayrıca, bulmayı zorlaştırmak için varsayılan SSID'yi değiştirmenizi de önemle tavsiye ederiz.

Wireless LAN >> General Setup

General Setting (IEEE 802.11)

<input checked="" type="checkbox"/>	Enable Wireless LAN				
	Mode :		Mixed(11b+11g+11n)		
	Channel:		Channel 6, 2437MHz		
	Enable	Hide SSID	SSID	Isolate Member	Isolate VPN
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	FAQTest	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	DrayTek_Guest	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

MAC Adresini Filtreleme

Yetkisiz cihazların AP'nize bağlanmasını önlemek için, White List policy ile Access Control'u etkinleştirebilirsiniz. MAC Adres Filtering List'e yalnızca yetkili cihazları ekleyin, diğer cihazlar engellenecektir. Veya, bir Wireless Repeater'in AP'nize bağlanmasını önlemek için, Black List Access Control Policy'i kullanabilir, bir AP Discovery taraması yapabilir ve yakındaki tüm AP'lerin MAC Adresini Black List'e ekleyebilirsiniz.

Wireless LAN >> Access Control

Access Control

Enable Mac Address Filter SSID 1 White List SSID 2 White List SSID 3 White List SSID 4 White List

MAC Address Filter(Limit: 64 entries)

Index	Attribute	MAC Address	Apply SSID
1		00:0C:20:99:3E:74	SSID1

Client's MAC Address : 00 : 1D : AA : 39 : 54 : 54

Apply SSID : SSID 1 SSID 2 SSID 3 SSID 4

Attribute : s: Isolate the station from LAN

DHCP Sunucusunu Devre Dışı Bırak

Ağınızdaki DHCP Server'i kapatın, böylece Client'in networke erişmek için statik bir IP adresi yapılandırması gerekir.

Misafirler için Ayrı Bir Ağ Oluşturun

Ziyaretçilerinize Wi-Fi bağlantı sağlamanız gerekiyorsa ve bağlantılarının kolay olmasını istiyorsanız, Router üzerinde başka bir VLAN oluşturun ve ziyaretçiler için ikinci bir SSID oluşturun, ve private networkü güvende tutun.

Wireless LAN (2.4GHz) >> General Setup

General Setting (IEEE 802.11)

Enable Wireless LAN

Enable Limit Client (3-64) (default: 64)

Mode :

Enable 2 Subnet (Simulate 2 APs)

	Hide SSID	SSID	Subnet	Isolate Member(0: Untagged)	VLAN ID	IGMP Snooping	Mac Clone
1	<input type="checkbox"/>	DrayTek-Staff	LAN-A	<input type="checkbox"/>	10	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	DrayTek-Guest	LAN-A	<input type="checkbox"/>	20	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>		LAN-A	<input type="checkbox"/>	0	<input type="checkbox"/>	<input type="checkbox"/>