What Is a Service Set Identifier (SSID)?

All wireless networks have their own network name

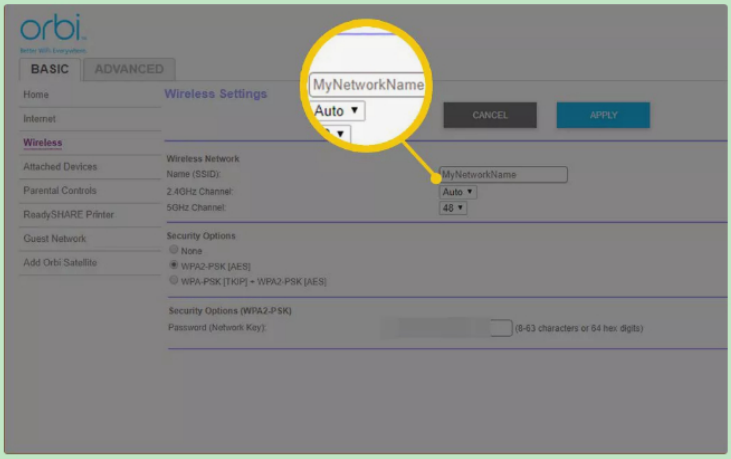
by Bradley Mitchell
reviewed by Michael Barton Heine Jr

Updated on April 17, 2020

The Wireless Connection

+ All About Wireless
+ How To Connect At Home
  - How to Name Your Wireless Network
  - How to Change Your Wireless Router's Admin Password
  - Change the Wi-Fi Channel Number to Avoid Interference
  - Build a Wireless Home Network
  - Use Wireless Speakers In Home Theater
  - Connect Your Echo & Alexa To Wi-Fi
  - Connect Google Home to Wi-Fi
  - Wirelessly Connect An iPad To Your TV
  - Use a Free Firewall Program
+ How To Connect On The Go
+ How to Troubleshoot Wireless Issues
+ The Future of Wireless

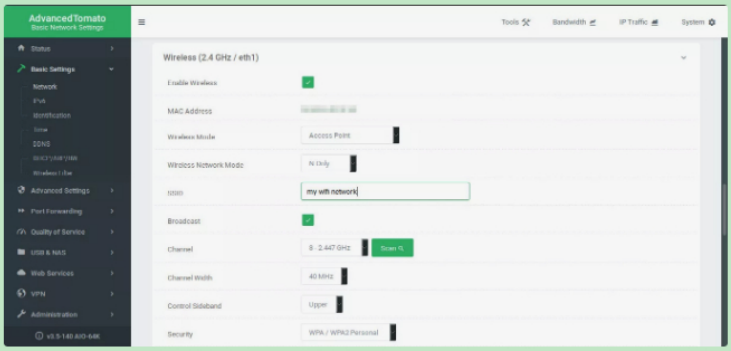
An SSID (service set identifier) is the primary name associated with an 802.11 wireless local area network (WLAN), including home networks and public hotspots. Client devices use this name to identify and join wireless networks. In simple terms, it's the name of your Wi-Fi network.



What an SSID Looks Like

The SSID is a case-sensitive text string that is as long as 32 characters consisting of letters and numbers. Within those rules, the SSID can say anything.

When you connect to a wireless network, you see your network and others within your range that are called something different. All of the names you see are the SSIDs for those networks.



Router manufacturers set a default SSID for the Wi-Fi unit, such as Linksys, xfinitywifi, NETGEAR, dlink, or default. However, since the SSID can be changed, not all wireless networks have a standard name.

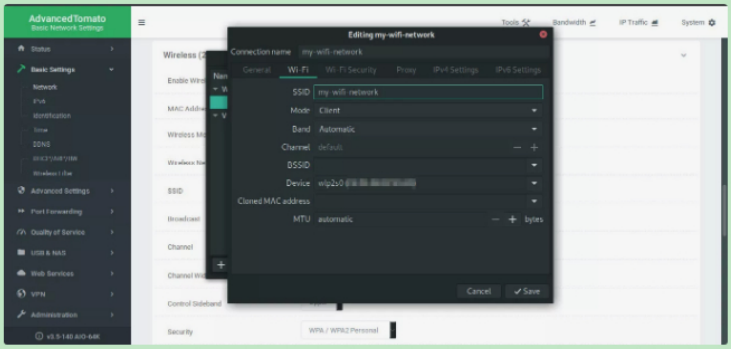
On home Wi-Fi networks, a broadband router or broadband modem stores the SSID, but administrators can change it. Routers broadcast this name to help wireless clients find the network.

wireless clients find the network.

How Devices Use SSIDs

Wireless devices like phones and laptops scan the local area for networks that broadcast their SSIDs and present a list of names. A user can initiate a new network connection by picking a name from the list.

In addition to obtaining the network name, a Wi-Fi scan also determines whether each network has wireless security options enabled. In most cases, the device identifies a secured network with a lock symbol next to the SSID.



Most wireless devices keep track of the networks a user joins as well as the connection preferences. In particular, users can set up a device to automatically join networks having certain SSIDs by saving that setting in their profiles.

In other words, once connected, the device usually asks if you want to save the network or reconnect automatically in the future. Also, you can set up the connection manually without having access to the network (you can connect to the network from afar so that when in range, the device knows how to log in).

Most wireless routers offer the option to disable SSID broadcasting as a means to improve Wi-Fi network security since it requires the clients to know two passwords: the SSID and the network password. However, the effectiveness of this technique is limited since it's easy to sniff out the SSID from the header of data packets flowing through the router.

Connecting to networks with SSID broadcast disabled requires the user to manually create a profile with the name and other connection parameters.

Issues With SSIDs

Consider these ramifications of how wireless network names work:

- If a network does not have wireless security options enabled, anyone can connect to it by knowing only the SSID.
- Using a default SSID increases the likelihood that another nearby network will have the same name, confusing wireless clients. When a Wi-Fi device discovers two networks with the same name, it may auto-connect to the one that has a stronger radio signal, which might be the unwanted choice. In the worst case, a person might get dropped from their home network and reconnected to a neighbor's network that doesn't have login protection enabled.
- The SSID chosen for a home network should contain only generic information. Some names (like HackMeIfYouCan) unnecessarily entice thieves to target certain homes and networks over others.
- An SSID can contain publicly-visible offensive language or coded messages.

Was this page helpful? 👍 👎 **Join the discussion** 0 Comment

The Wireless Connection
NEXT UP:
How to Change Your Wireless Router's Admin Password ➔

More from Lifewire

Wi-Fi & Wireless

How to Set up Your Home Wi-Fi Network

Wi-Fi & Wireless

How to Troubleshoot When You Have No Wireless Connection

Routers & Firewalls

Disable SSID Broadcast to Hide Your Wi-Fi Network

Android

How to Connect Your Android Device to Wi-Fi

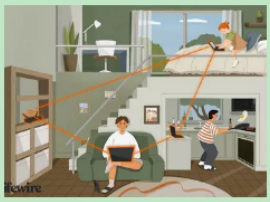
Home Networking

Top 10 Tips for Wireless Home Network Security

Routers & Firewalls

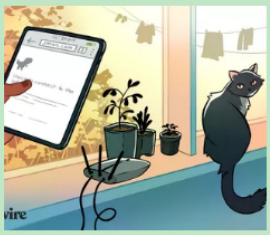
A Guide to Changing the Wi-Fi Name (SSID) on a Network Router

Home Networking



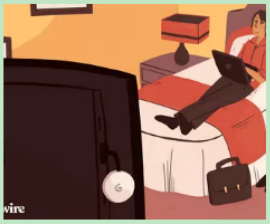
How to Build a Wireless Home Network

iPad



How to Fix an iPad That Won't Connect to Wi-Fi

Chromecast



How to Use Chromecast Without Wi-Fi

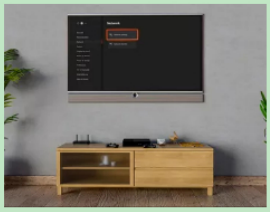
Routers & Firewalls

Should You Change the Default Name (SSID) of a Wireless Router?

Wi-Fi & Wireless

How to Stop People From Using Your Wi-Fi

Consoles & PCs



How to Fix an Xbox That Won't Connect to Wi-Fi

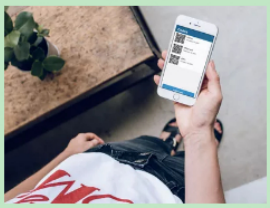
Home Networking

How to Set Up A Modem

Wi-Fi & Wireless

Understanding Wi-Fi and How It Works

Android



How to Share a Wi-Fi Password From iPhone to Android

Wi-Fi & Wireless

5 Tips for Securing Your Wireless Network

Lifewire

Get the Latest Tech News Delivered Every Day

email address

enter

Follow Us Facebook

News

Best Products

Mobile Phones

Computers

About Us
Advertise
Privacy Policy
Cookie Policy
Careers
Editorial Guidelines
Contact
Terms of Use
California Privacy Notice

.dash Lifewire is part of the Dotdash publishing family.