SOPHOS

Security made simple.

Sophos Central

SSIDs

Product Version 1.15

Contents

1 About SSIDs

A Service Set Identifier (SSID) is a unique identifier which is attached to the header of packets that are sent over a Wireless LAN. It differentiates one WLAN from another. Multiple access points within a network can use the same SSID to broadcast the same network. You can also have multiple SSIDs on an access point. This allows you to have SSIDs with different bands or other configurations like separate guest networks or a mesh network.

SOS SSID

When an access point is disconnected or not able to reach Sophos Central, the access point will use its wireless capability to create an SOS SSID. When you connect to the SOS SSID with any mobile device you receive information about the current state of an access point which can help you debug the connection issues to Sophos Central.

The SOS SSID is comprised of an open wireless network named "sos" and the access point's MAC address. After you connected to the SOS SSID, open your web browser and navigate to *http://debug.sophos*. The SOS SSID debug page provides the technical support to fix the connection issue, for example:

- Serial number and MAC address of the access point's Ethernet interface
- Link status
- IP of the access points Ethernet interface
- Gateway, DNS server and their reachability
- Reachability of Sophos Central URLs

Note: The SOS SSID is available for a limited time frame of four minutes. After that, the access point reboots and the SOS SSID is available again after one or two minutes. When you are connected to an SOS SSID, you have no access to the internet.

2 Security and Quality of Service settings

SSIDs can be secured and improved in terms of quality with some options in Sophos Central.

Security features

Hidden SSID	When hidden, the SSID is still available but users needs to know the name to connect directly. Even if an SSID is hidden, you can assign the SSID to an access point. **Note:** This is not a security feature. You still need to protect hidden SSIDs.
Client isolation	Clients within the same radio are not allowed to communicate with one another. This could be useful, for example in a guest or hotspot network.
MAC Filtering	Provides minimal security by restricting MAC address connections. ▪ **Blocked List**: All MAC addresses are allowed except the ones you enter in the MAC addresses field. ▪ **Allowed List**: All MAC addresses are prohibited except the ones you enter in the MAC addresses field.

Quality of Service features

Multicast to unicast conversion	The access point converts multicast packets to unicast packets individually for each client based on the IGMP protocol. This approach is more powerful when few clients are connected to one access point. Unicast is preferred to multicast in most scenarios where media is streamed as it can operate at higher rates.
Proxy ARP	If activated, the AP can answer ARP queries for network addresses directly and the other clients do not need to take action.

Fast roaming	SSIDs with WPA2 encryption use the IEEE 802.11r standard to reduce roaming times (with enterprise authentification). It applies when the same SSID is assigned to different access points. Clients also need to support the IEEE 802.11r standard.
Keep broadcasting	Ensures that the access point keeps broadcasting when it is not able to re-connect to Sophos Central after a reboot. With this function, clients will still be able to connect to the access point and/or the internet. If the keep broadcasting function is on, the access point proceeds working with its old configuration. **Note:** The SSID will be broadcasted in all cases of connection loss to Sophos Central, regardless if this function is activated or not.
Band Steering	Band steering distributes clients based on the load of the two bands and the clients' capability between 2.4 GHz and 5 GHz bands. Dual-band capable wireless clients will be routed to 5 GHz if possible to improve the client experience. This is done by rejecting the initial association request sent by the client in the 2.4 GHz band. This will cause dual-band devices to then attempt to negotiate at 5 GHz. If it does not associate in the 5 GHz band, it will be marked as "steering unfriendly" and will not be routed again. If a client is too far away from the AP, routing will not be attempted. This prevents routing clients to 5 GHz when the range is usually less than in the 2.4 GHz band. Band Steering is done on a per-AP level and will affect all SSIDs on that AP.

3 Creating and activating an SSID

SSIDs can be very complex to create as there are a lot of configuration options.

Objectives

When you complete this lesson, you'll know how to do the following:

- Create an SSID and add it to access points
- Secure the SSID properly

3.1 Creating an SSID

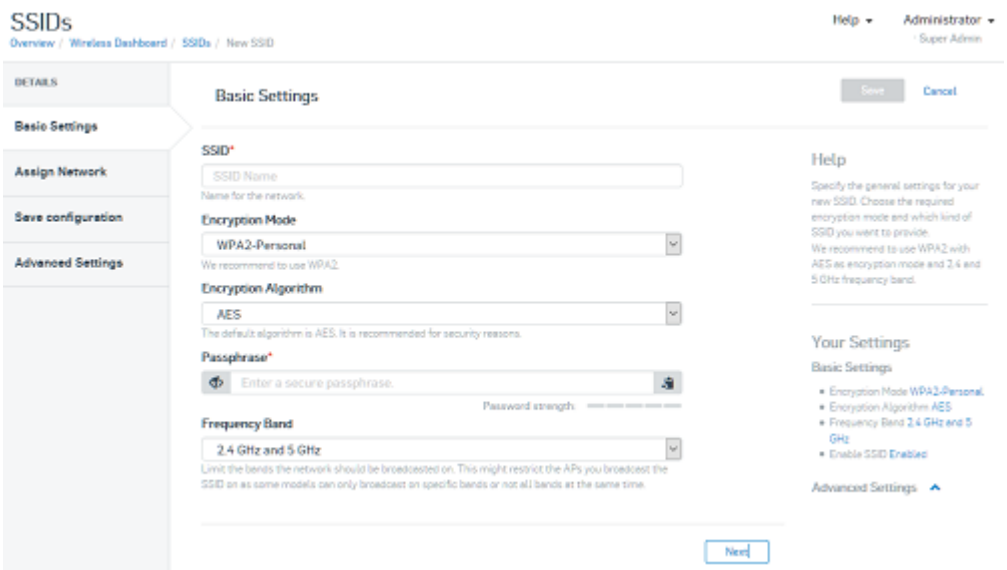
Before you begin

Before you start creating an SSID the following conditions should be met:

- You have an active Sophos Central Wireless license.
- We recommend having at least one access point registered before you create SSIDs.

Procedure

1. Go to **Wireless** > **SSIDs** and click **Create**.



2. Type a name for your SSID.

   This is the name of the network which will be displayed in the wireless network selection on your mobile device or laptop.

3. Type a secure passphrase.

   Use numbers, characters and special characters in combination.

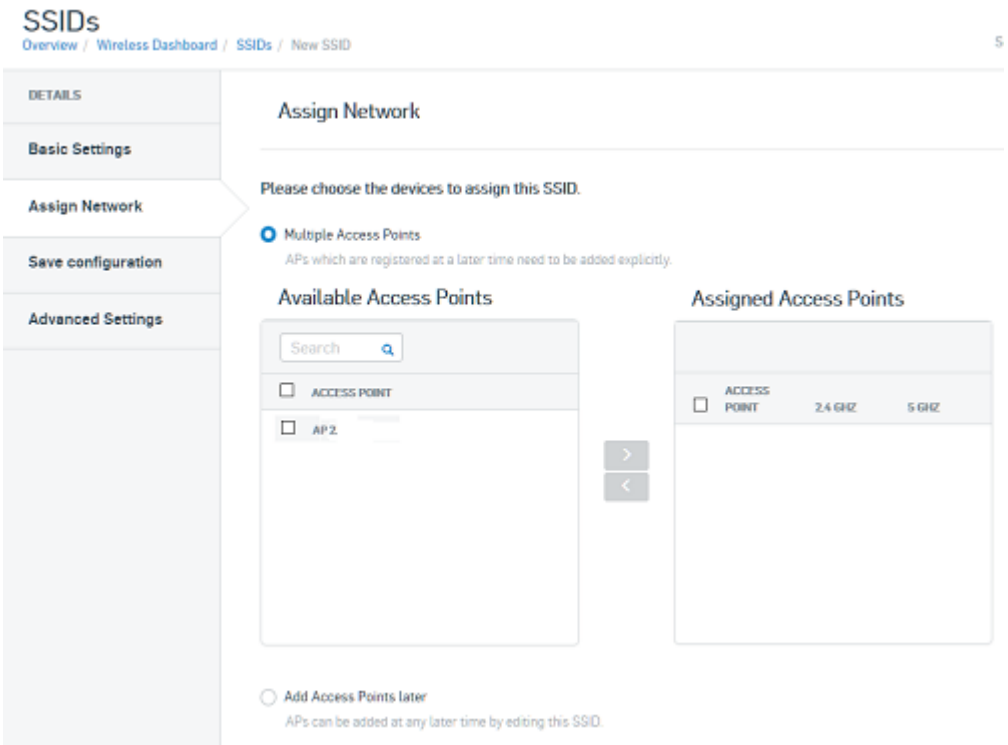
4. Select the frequency band according to your needs.

   Some APs do not support the 5 GHz band.

   Note: For more information on which access point types support the 5 GHz band, see Supported Access Points.

   For VoIP communication, the 5 GHz band should be preferred. It has higher performance, lower latency, and less interference.

5. Click **Next.**.
6. Click **Multiple Access Points**.



7. Select the desired APs and add them to the **Assigned Access Points** list.
8. Click **Next.**.

   You can now activate the SSID.

9. Save your settings.

Results

The SSID is now available and will be broadcasted on the selected access points.

What to do next

Proceed securing the SSID.

3.2 Securing an SSID

Before you begin

Ensure that you have an SSID created.

Procedure

1. Go to **SSIDs** and click on the desired SSID.
2. Go to **Advanced Settings** > **Security**.
3. Make the required settings.
4. Go to **Quality of Service** and make the required settings to improve the service quality.
5. Save your settings.