



Article ID: 5054

Configuring a Guest Wireless Network

Overview

Expanding your small business network with a Cisco Small Business Wireless Access Point is an excellent way to get your employees connected to the network from anywhere. Products like the WAP371 can easily be integrated into an existing network and provide the latest 802.11ac high-speed wireless connection. The Cisco wireless Guest Access feature offers the same mobility and convenience that is provided to employees to client and other visitors to the network.

The Cisco Wireless Guest Access feature provides a convenient, cost-effective way to offer wireless access to visitors while maintaining security on your internal network. Wireless guest networks provide the following basic functionality:

- Provides Internet access to guests through an open connection
- Traffic on the guest network is kept separate from the business network
- Wireless access for each guest is isolated to prevent guests from communicating with one another over the network.

Key Features

Inter-VLAN Routing

Combining the Inter-VLAN routing provided by a Cisco RV router with the wireless SSID isolation feature provided in a Cisco small business wireless access point offers a simple and secure solution for guest access on any existing Cisco small business network at no additional cost.

Wireless SSID Isolation

The Wireless SSID Isolation feature separates users on the Guest Wireless network from users on the normal wireless network. Additionally, by enabling Wireless Isolation (within SSID), wireless users on the Guest Network will be separated from each other as well. This allows you to provide your users with additional security.

802.1Q Encapsulation

The IEEE 802.1Q standard is used to handle transferring traffic from multiple VLANs over a single link (the “trunk”). When a packet is marked as “tagged”, it will be sent over the link with identifying information allowing the receiving end to identify which VLAN it belongs to. “Untagged” traffic is sent over the link with no identifying information. Traffic marked “Excluded” is not allowed to cross the link.

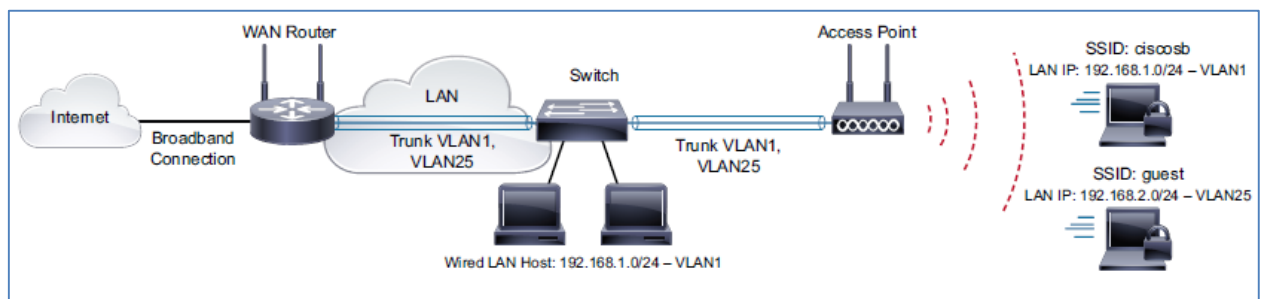
Devices Used

- RV130 Router (1.0.1.3)
- SG300 Series Gigabit PoE+ Managed Switch (1.4.0.88)
- WAP371 Wireless Access Point (1.1.2.3)

Note: The devices used are not the only ones applicable to this configuration. This setup may also apply to your network. Please consult the admin guides for your specific devices to determine if the Guest Network feature is available.

Note: The WAP371 requires an 802.3at compliant power source if it is to be powered over an Ethernet cable. This is available in all Cisco PoE+ switches or through the use of an 802.3at PoE injector.

Network Topology



For our scenario, we will have the WAN port of our RV130 plugged in to our broadband Internet connection, and Port 1 on the RV 130 plugged in to port G9 of our SG300. We will also have Port 1 on our SG300 plugged in to the Ethernet port of our WAP371. We will be using the 5GHz band on the WAP371 in order to take advantage of the higher bandwidth.

Adding and Configuring a Guest Access VLAN on the RV130

Step 1. Open the web configuration utility for your router and navigate to **Networking > LAN > VLAN Membership**. The *VLAN Membership* page open:

VLAN Membership

Create VLANs and assign the Outgoing Frame Type.
Up to four VLANs total can be created. VLAN IDs must be in the range (3 - 4094)

VLANs Setting Table						
Select	VLAN ID	Description	Port 1	Port 2	Port 3	Port 4
<input type="checkbox"/>	1	Default	Untagged	Untagged	Untagged	Untagged

Step 2. Click **Add Row** to add a new VLAN to the table. A new row will appear in the VLAN setting table.

VLAN Membership

Create VLANs and assign the Outgoing Frame Type.
Up to four VLANs total can be created. VLAN IDs must be in the range (3 - 4094)

VLANs Setting Table						
Select	VLAN ID	Description	Port 1	Port 2	Port 3	Port 4
<input type="checkbox"/>	1	Default	Untagged	Untagged	Untagged	Untagged

Step 3. Enter a number for your guest VLAN ID in the *VLAN ID* field. Remember this ID number as it will apply to settings on the switch and wireless access point as well. In this example VLAN ID 25 is chosen for the guest network.

VLAN Membership

Create VLANs and assign the Outgoing Frame Type.
Up to four VLANs total can be created. VLAN IDs must be in the range (3 - 4094)

You must save before you can edit or delete.

VLANs Setting Table			
Select	VLAN ID	Description	Port 1
<input type="checkbox"/>	1	Default	Untagged
<input type="checkbox"/>	25		Tagged ▼

Step 4. In the *Description* field, enter a name for the VLAN. Because this will be used for guest network access in this example, it has been named as *Guest*.

VLAN Membership

Create VLANs and assign the Outgoing Frame Type.
Up to four VLANs total can be created. VLAN IDs must be in the range (3 - 4094)

You must save before you can edit or delete.

VLANs Setting Table			
Select	VLAN ID	Description	Port 1
<input type="checkbox"/>	1	Default	Untagged
<input type="checkbox"/>	25	Guest	Tagged ▼

Step 5. For the drop-down lists for each port, select **Tagged** for the port connecting the router to the switch. This will mark packets from the guest VLAN so they can be identified by the other device on the receiving end. For all other unconnected ports, select **Excluded** to block traffic from the guest VLAN going to these ports. In this example the RV130 is connected to the SG300 through LAN port 1. For additional

information regarding “tagged” and “untagged” traffic, refer to [802.1Q Encapsulation](#) in the *Key Features* section of this document.

VLAN Membership

Create VLANs and assign the Outgoing Frame Type.
Up to four VLANs total can be created. VLAN IDs must be in the range (3 - 4094)

You must save before you can edit or delete.

Select	VLAN ID	Description	Port 1	Port 2	Port 3	Port 4
<input type="checkbox"/>	1	Default	Untagged	Untagged	Untagged	Untagged
<input type="checkbox"/>	25	Guest	Tagged ▼	Excluded ▼	Excluded ▼	Excluded ▼

Step 6. Click **Save** to save your newly created guest VLAN.

VLAN Membership

Create VLANs and assign the Outgoing Frame Type.
Up to four VLANs total can be created. VLAN IDs must be in the range (3 - 4094)

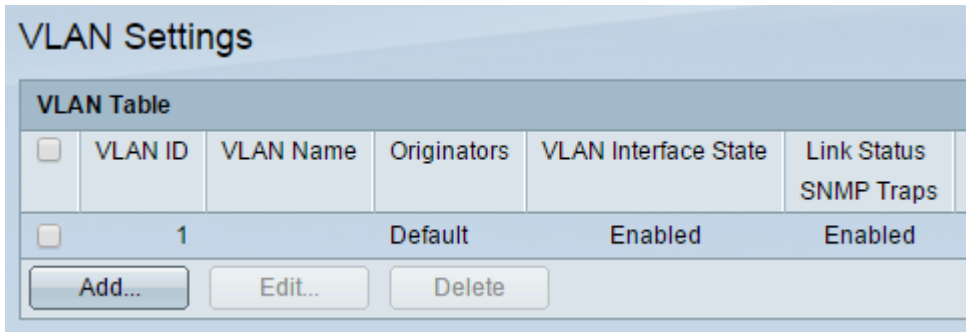
You must save before you can edit or delete.

Select	VLAN ID	Description	Port 1	Port 2	Port 3	Port 4
<input type="checkbox"/>	1	Default	Untagged	Untagged	Untagged	Untagged
<input type="checkbox"/>	25	Guest	Tagged ▼	Excluded ▼	Excluded ▼	Excluded ▼

Adding and Configuring a Guest Access VLAN on the SG300

In this section, guest access VLAN 25 will be added to the SG300 switch and the VLAN will be included on its trunk to the router. Skip to [Adding and Configuring a Guest Access VLAN on the WAP371](#) if you plan to connect your wireless access point directly to the RV130 router.

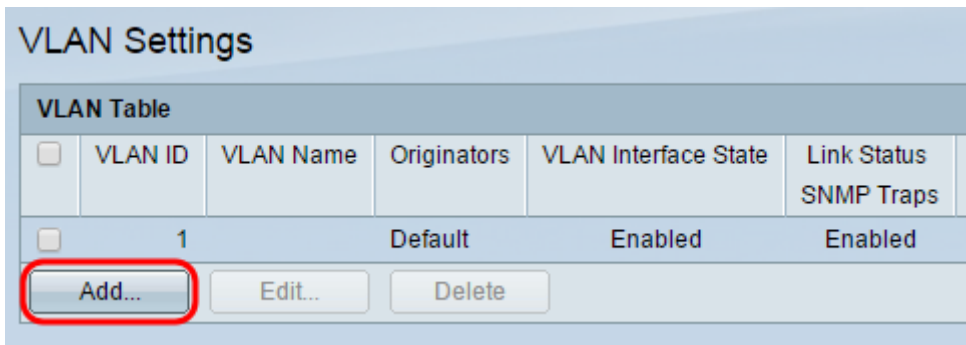
Step 1. Login to the web configuration utility of the SG300 and navigate to **VLAN Management > VLAN Settings**. The *VLAN Settings* page appears:



VLAN Settings

VLAN Table					
<input type="checkbox"/>	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
<input type="checkbox"/>	1	Default		Enabled	Enabled

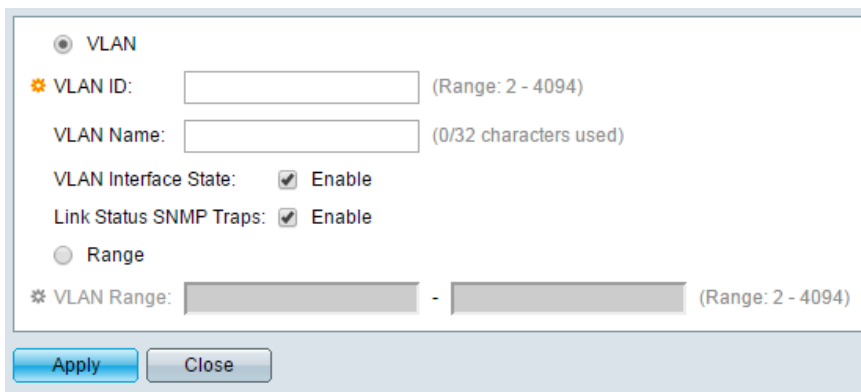
Step 2. Click **Add...** to add a new VLAN.



VLAN Settings

VLAN Table					
<input type="checkbox"/>	VLAN ID	VLAN Name	Originators	VLAN Interface State	Link Status SNMP Traps
<input type="checkbox"/>	1	Default		Enabled	Enabled

The *Add VLAN* window appears:



VLAN

* VLAN ID: (Range: 2 - 4094)

VLAN Name: (0/32 characters used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

* VLAN Range: - (Range: 2 - 4094)

Step 3. In the *VLAN ID* field, enter the ID of the VLAN that will be used for guest network access. Make sure that the ID matches the ID set on the router in the previous section.

VLAN

VLAN ID: 25 (Range: 2 - 4094)

VLAN Name: (0/32 characters used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

* VLAN Range: - (Range: 2 - 4094)

Apply Close

Step 4. In the *VLAN Name* field, enter a name for the guest VLAN.

VLAN

VLAN ID: 25 (Range: 2 - 4094)

VLAN Name: Guest (5/32 characters used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

* VLAN Range: - (Range: 2 - 4094)

Apply Close

Step 5. In the *VLAN Interface State* field, select the check box to enable the VLAN Interface inside the switch.

VLAN

VLAN ID: 25 (Range: 2 - 4094)

VLAN Name: Guest (5/32 Characters Used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

* VLAN Range: - (Range: 2 - 4094)

Apply Close

Step 6. (Optional) In the *Link Status SNMP Traps* field, select the checkbox to allow the switch to send SNMP Traps relating to the operational status of this VLAN. Simple Network Management Protocol (SNMP) Traps are messages that the switch can be configured to send to a SNMP Management Program when events occur, allowing a network administrator to have a centralized database containing information that is updated in real-time.

VLAN

VLAN ID: 25 (Range: 2 - 4094)

VLAN Name: Guest (5/32 Characters Used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

* VLAN Range: - (Range: 2 - 4094)

Apply Close

Step 7. Now click **Apply**. The newly created VLAN should appear in the table.

VLAN

VLAN ID: 25 (Range: 2 - 4094)

VLAN Name: Guest (5/32 characters used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

* VLAN Range: - (Range: 2 - 4094)

Apply Close

Step 8. Click **Close** to close the *ADD VLAN* window.

Success. To permanently save the configuration, go to the [Copy/Save Configuration](#) page or click the Save icon.

VLAN

VLAN ID: (Range: 2 - 4094)

VLAN Name: (0/32 characters used)

VLAN Interface State: Enable

Link Status SNMP Traps: Enable

Range

* VLAN Range: - (Range: 2 - 4094)

Step 9. Navigate to **VLAN Management > Port to VLAN**. The *Port to VLAN* page appears:

Port to VLAN

VLAN Membership Table

Filter: VLAN ID equals to ▼

AND Interface Type equals to ▼

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Trunk	<input type="text" value="Untagged"/> ▼	<input checked="" type="checkbox"/>
GE2	Trunk	<input type="text" value="Untagged"/> ▼	<input checked="" type="checkbox"/>
GE3	Trunk	<input type="text" value="Untagged"/> ▼	<input checked="" type="checkbox"/>
GE4	Trunk	<input type="text" value="Untagged"/> ▼	<input checked="" type="checkbox"/>
GE5	Trunk	<input type="text" value="Untagged"/> ▼	<input checked="" type="checkbox"/>
GE6	Trunk	<input type="text" value="Untagged"/> ▼	<input checked="" type="checkbox"/>
GE7	Trunk	<input type="text" value="Untagged"/> ▼	<input checked="" type="checkbox"/>
GE8	Trunk	<input type="text" value="Untagged"/> ▼	<input checked="" type="checkbox"/>
GE9	Trunk	<input type="text" value="Untagged"/> ▼	<input checked="" type="checkbox"/>
GE10	Trunk	<input type="text" value="Untagged"/> ▼	<input checked="" type="checkbox"/>

Step 10. From the *VLAN ID equals to* drop-down list, select the ID of the guest network.

Port to VLAN

VLAN Membership Table

Filter: VLAN ID equals to

AND Interface Type equals to

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE2	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE3	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE4	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE5	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE6	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE7	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE8	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE9	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE10	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>

Step 11. Click **Go**. The *VLAN Membership* table for the guest VLAN is displayed below.

VLAN Membership Table

Filter: VLAN ID equals to

AND Interface Type equals to

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE2	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE3	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE4	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE5	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE6	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE7	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE8	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE9	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>
GE10	Trunk	Untagged <input type="button" value="v"/>	<input checked="" type="checkbox"/>

Step 12. For each of the port interfaces of the switch listed in the table, choose the appropriate membership type from the drop-down list. The ports which connect the switch to both the WAP371 (GE1) and the RV130 (GE9) should be Tagged to mark the packets to be identified on the receiving end, while all other unconnected ports for the guest VLAN should be set to Excluded to block guest traffic from entering.

Port to VLAN

VLAN Membership Table

Filter: VLAN ID equals to

AND Interface Type equals to

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Trunk	Tagged <input type="button" value="v"/>	<input type="checkbox"/>
GE2	Trunk	Excluded <input type="button" value="v"/>	<input type="checkbox"/>
GE3	Trunk	Excluded <input type="button" value="v"/>	<input type="checkbox"/>
GE4	Trunk	Excluded <input type="button" value="v"/>	<input type="checkbox"/>
GE5	Trunk	Excluded <input type="button" value="v"/>	<input type="checkbox"/>
GE6	Trunk	Excluded <input type="button" value="v"/>	<input type="checkbox"/>
GE7	Trunk	Excluded <input type="button" value="v"/>	<input type="checkbox"/>
GE8	Trunk	Excluded <input type="button" value="v"/>	<input type="checkbox"/>
GE9	Trunk	Tagged <input type="button" value="v"/>	<input type="checkbox"/>
GE10	Trunk	Excluded <input type="button" value="v"/>	<input type="checkbox"/>

Step 13. Click **Apply** to save the settings.

VLAN Membership Table

Filter: VLAN ID equals to

AND Interface Type equals to

Interface Name	VLAN Mode	Membership Type	PVID
GE1	Trunk	<input type="text" value="Tagged"/> <input type="button" value="v"/>	<input type="checkbox"/>
GE2	Trunk	<input type="text" value="Excluded"/> <input type="button" value="v"/>	<input type="checkbox"/>
GE3	Trunk	<input type="text" value="Excluded"/> <input type="button" value="v"/>	<input type="checkbox"/>
GE4	Trunk	<input type="text" value="Excluded"/> <input type="button" value="v"/>	<input type="checkbox"/>
GE5	Trunk	<input type="text" value="Excluded"/> <input type="button" value="v"/>	<input type="checkbox"/>
GE6	Trunk	<input type="text" value="Excluded"/> <input type="button" value="v"/>	<input type="checkbox"/>
GE7	Trunk	<input type="text" value="Excluded"/> <input type="button" value="v"/>	<input type="checkbox"/>
GE8	Trunk	<input type="text" value="Excluded"/> <input type="button" value="v"/>	<input type="checkbox"/>
GE9	Trunk	<input type="text" value="Tagged"/> <input type="button" value="v"/>	<input type="checkbox"/>
GE10	Trunk	<input type="text" value="Excluded"/> <input type="button" value="v"/>	<input type="checkbox"/>

Step 14. Navigate to **Administration > File Management > Copy/Save Configuration**. The *Copy/Save Configuration* page appears:

Copy/Save Configuration

All configurations that the switch is currently using are in the running configuration file which is volatile and is not retained between reboots. To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you have completed all your changes.

Source File Name: Running configuration
 Startup configuration
 Backup configuration
 Mirror configuration

Destination File Name: Running configuration
 Startup configuration
 Backup configuration

Sensitive Data: Exclude
 Encrypted
 Plaintext
Available sensitive data options are determined by the current user's SSD rules

Save Icon Blinking: Enabled

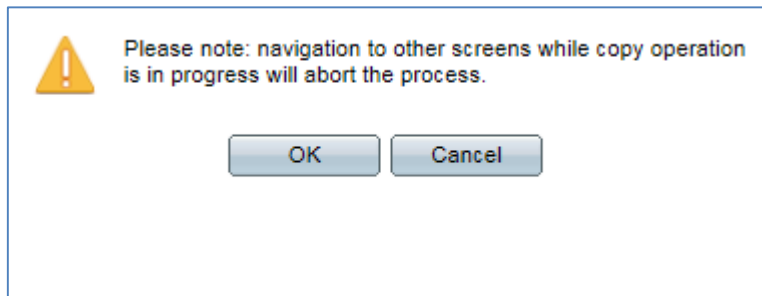
Step 15. Click **Apply** to save the configuration. For additional information on the fields presented on this page, refer to [Download/Backup Configuration on the WAP371](#).

Copy/Save Configuration

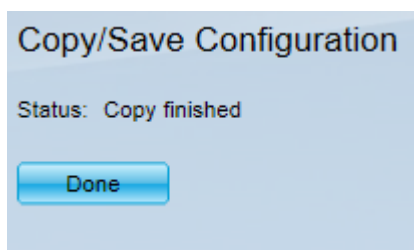
All configurations that the switch is currently using are in the running configuration file which is volatile and is not retained between reboots. To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you have completed all your changes.

Source File Name:	<input checked="" type="radio"/> Running configuration
	<input type="radio"/> Startup configuration
	<input type="radio"/> Backup configuration
	<input type="radio"/> Mirror configuration
Destination File Name:	<input type="radio"/> Running configuration
	<input checked="" type="radio"/> Startup configuration
	<input type="radio"/> Backup configuration
Sensitive Data:	<input type="radio"/> Exclude
	<input checked="" type="radio"/> Encrypted
	<input type="radio"/> Plaintext
	<small>Available sensitive data options are determined by the current user's SSD rules</small>
Save Icon Blinking:	Enabled

The *Copy File* dialog box appears:



Step 16. Click **OK**. The *Copy/Save Configuration Status Page* appears:



Step 17. Click **Done**.

Adding and Configuring a Guest Access VLAN on the WAP371

In this section, a separate SSID is created for guest access and security settings are applied to the wireless network.

Enable the Wireless Radio

Step 1. Log in to your wireless access point web configuration utility and navigate to **Wireless > Radio**. The *Radio* page appears:

Radio

Global Settings

TSPEC Violation Interval: Sec (Range: 0 - 900, 0 = Disable, Default: 300)

Radio Setting Per Interface

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Basic Settings

Radio: Enable

MAC Address: 7C:69:F6:35:95:B0

Mode: ▼

Channel Bandwidth: ▼

Primary Channel: ▼

Channel: ▼

Step 2. Select the radio button for the wireless radio you would like to enable. The 2.4Ghz band is widely supported. The 5Ghz band is not supported by all devices and has a smaller range, but supports higher speeds.

Radio

Global Settings

TSPEC Violation Interval: Sec (Range: 0 - 900, 0 = Disable, Default: 300)

Radio Setting Per Interface

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Basic Settings

Radio: Enable

MAC Address: 7C:69:F6:35:95:B0

Mode: ▼

Channel Bandwidth: ▼

Primary Channel: ▼

Channel: ▼

Step 3. Check the **Enable** check box in the *Radio* field to enable the use of the wireless radio. If you are enabling the 5GHz radio, a pop up message will appear notifying you that an 802.3at compliant power source is required. Normal PoE does not support the 802.3at standard. PoE+ devices and the AC Adapter meet the 802.3at standard. Click **OK** to continue.

Radio

Global Settings

TSPEC Violation Interval: Sec (Range: 0 - 900, 0 = Disable)

Radio Setting Per Interface

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Basic Settings

Radio: Enable

MAC Address: 7C:69:F6:35:95:B0

Mode: ▼

Channel Bandwidth: ▼

Step 4. Click **Save** to apply the changes.

Status and Statistics
 Administration
 LAN
 Wireless
 Radio
 Rogue AP Detection
 Networks
 Scheduler
 Scheduler Association
 Bandwidth Utilization
 MAC Filtering
 WDS Bridge
 WorkGroup Bridge
 QoS
 System Security
 Client QoS
 SNMP
 Single Point Setup
 Captive Portal

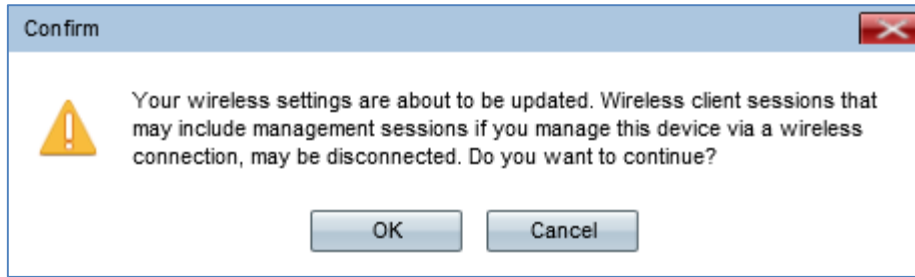
Transmit Power: ▼
Frame-burst Support: ▼ [Boosts Downstream Throughput]
Fixed Multicast Rate: ▼ Mbps
Legacy Rate Sets:

Rate (Mbps)	54	48	36	24	18	12	9	6
Supported	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Basic	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Broadcast/Multicast Rate Limiting
Rate Limit: Packets Per Second (Range: 1 - 50, Default: 50)
Rate Limit Burst: Packets Per Second (Range: 1 - 75, Default: 75)

TSPEC Mode: ▼
TSPEC Voice ACM Mode: ▼
TSPEC Voice ACM Limit: Percent (Range: 0 - 70, Default: 20)
TSPEC Video ACM Mode: ▼
TSPEC Video ACM Limit: Percent (Range: 0 - 70, Default: 15)
TSPEC AP Inactivity Timeout: Sec (Range: 0 - 120, 0 = Disable, Default: 30)
TSPEC Station Inactivity Timeout: Sec (Range: 0 - 120, 0 = Disable, Default: 30)
TSPEC Legacy WMM Queue Map Mode: ▼

A confirmation window will appear:



Step 5. Click **OK** to continue. The page will refresh.

Assign the VLANs to SSIDs

Step 1. Log in to your wireless access point web configuration utility and navigate to **Wireless > Networks**. The *Network* page appears:

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Add Edit Delete

Save

Step 2. In the *Radio* field, choose the radio button that corresponds to the radio you would like to set up for use in wireless guest access. This should match the radio that you previously enabled in step 2 of the previous section.

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>

Add Edit Delete

Save

Step 3. Select the check box next to the SSID with VLAN ID 1 and click **Edit**. This allows changes to be made to the fields corresponding with the VLAN for internal use.

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Add Edit Delete

Save

Step 4. Enter in a name for your internal network in the *SSID Name* field.

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	discost	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Add Edit Delete

Save

Step 5. To add a secure password to your wireless network for internal use, select **WPA Personal** from the *Security* drop-down list. A new menu of options appears:

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Hide Details

WPA Versions: WPA-TKIP WPA2-AES
 Key: (Range: 8-63 Characters)
 Show Key as Clear Text
 Key Strength Meter: ■■■ Below Minimum
 Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)

Add Edit Delete

Save

Note: WPA Enterprise is a more advanced security option that offers logging of individual users through a centralized RADIUS server. For more information on WPA Enterprise configuration, refer to [Configuring WPA Enterprise on the WAP371](#).

Step 6. In the *Key* field, enter the desired password for your wireless access. The Key Strength Meter evaluates the strength of your chosen password against possible security threats.

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Hide Details

WPA Versions: WPA-TKIP WPA2-AES

Key: [Redacted] (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: [Redacted] Strong

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Add Edit Delete

Save

Step 7. To add the guest SSID, click **Add**. A new entry in the SSID list appears.

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
1	<input type="checkbox"/>			<input type="checkbox"/>			<input type="checkbox"/>	<input type="checkbox"/>	

Hide Details

WPA Versions: WPA-TKIP WPA2-AES

Key: [Redacted] (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: [Redacted] Strong

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Add Edit Delete

Save

Step 8. To begin setting up the guest SSID, select its check box and click **Edit**.

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
1	<input checked="" type="checkbox"/>			<input type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Hide Details

WPA Versions: WPA-TKIP WPA2-AES

Key: [Redacted] (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: [Redacted] Strong

Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

Add Edit Delete

Save

Step 9. In the *VLAN ID* field, enter in the ID associated with the guest VLAN in your network. Make sure this ID matches the one you have chosen during the configuration of your router and switch.

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
Hide Details									
WPA Versions: <input checked="" type="checkbox"/> WPA-TKIP <input checked="" type="checkbox"/> WPA2-AES Key: <input type="text" value="....."/> (Range: 8-63 Characters) <input type="checkbox"/> Show Key as Clear Text Key Strength Meter: <input type="text" value="Strong"/> Broadcast Key Refresh Rate: <input type="text" value="300"/> Sec (Range: 0-86400, 0 = Disable, Default: 300)									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	25		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Add Edit Delete

Save

Step 10. Enter in a name for your guest network in the *SSID Name* field.

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
Hide Details									
WPA Versions: <input checked="" type="checkbox"/> WPA-TKIP <input checked="" type="checkbox"/> WPA2-AES Key: <input type="text" value="....."/> (Range: 8-63 Characters) <input type="checkbox"/> Show Key as Clear Text Key Strength Meter: <input type="text" value="Strong"/> Broadcast Key Refresh Rate: <input type="text" value="300"/> Sec (Range: 0-86400, 0 = Disable, Default: 300)									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	25	Guest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	

Add Edit Delete

Save

Step 11. To prevent guest network users from being able to directly communicate over the local network, check the *Channel Isolation* check box.

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
Hide Details									
WPA Versions: <input checked="" type="checkbox"/> WPA-TKIP <input checked="" type="checkbox"/> WPA2-AES Key: <input type="text" value="....."/> (Range: 8-63 Characters) <input type="checkbox"/> Show Key as Clear Text Key Strength Meter: <input type="text" value="Strong"/> Broadcast Key Refresh Rate: <input type="text" value="300"/> Sec (Range: 0-86400, 0 = Disable, Default: 300)									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	25	Guest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Add Edit Delete


Save

Step 12. Click **Save** to save the newly configured SSIDs.

Networks

Select the radio interface first, and then enter the configuration parameters.

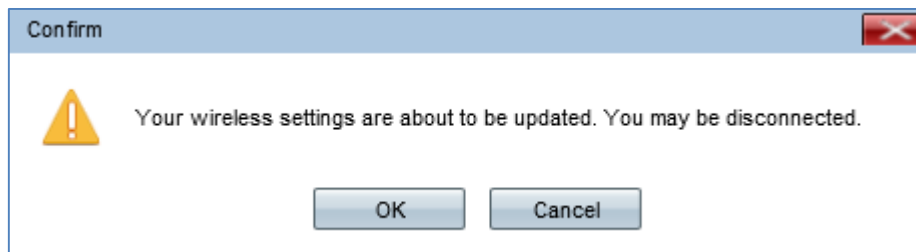
Radio: Radio 1 (5 GHz)
 Radio 2 (2.4 GHz)

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>	
Hide Details									
WPA Versions: <input checked="" type="checkbox"/> WPA-TKIP <input checked="" type="checkbox"/> WPA2-AES Key: <input type="text" value="....."/> (Range: 8-63 Characters) <input type="checkbox"/> Show Key as Clear Text Key Strength Meter:  Strong Broadcast Key Refresh Rate: <input type="text" value="300"/> Sec (Range: 0-86400, 0 = Disable, Default: 300)									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	25	Guest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Add Edit Delete

Save

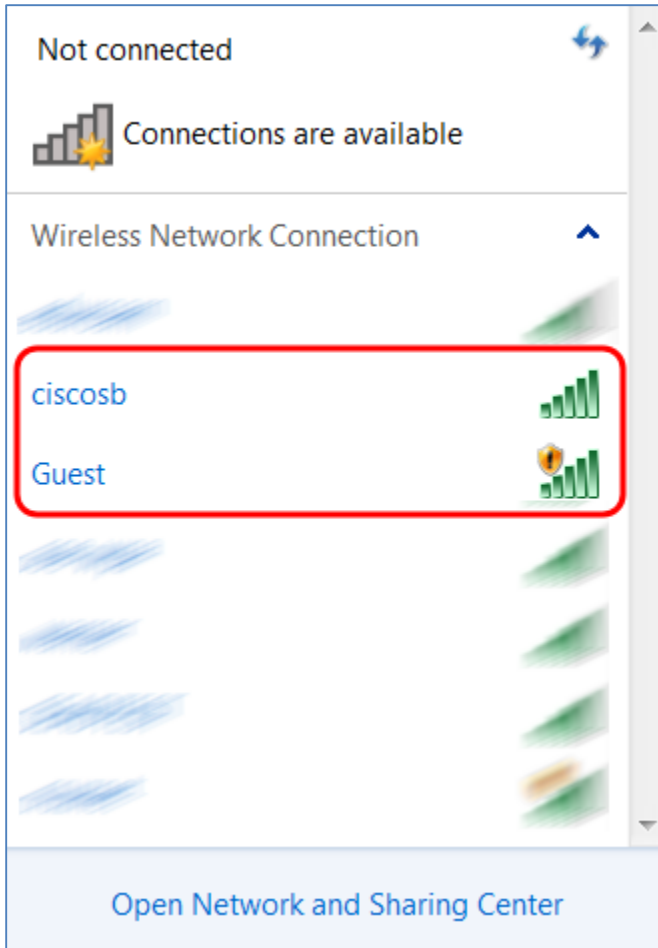
The *Confirm* window appears:



Step 13. Click **OK** to continue.

Verifying SSIDs

You should now see 2 new wireless networks with the SSIDs that you configured in the *Assigning VLANs to SSIDs* subsection of *Adding and Configuring a Guest Access VLAN on the WAP371* in this article.



Other Considerations

Managing Wireless Guest Access

Advanced Wireless Guest Access features can redirect guests to a captive portal page in their web browser requiring a username and password login. It can also include information and require users to consent to terms and conditions to continue. In order to learn more about setting up your own captive portal with advanced guest access features, refer to [Configuring Captive Portal on the WAP351 and WAP371 Access Points](#).