



print



email

**Article ID: 4937**

# **Enable a Captive Portal on your Cisco Wireless Network**

## **Enabling Captive Portal on your Cisco Wireless Network**

In an increasingly mobile, collaborative business environment, more organizations are opening up their network environments for controlled sharing of resources with business partners, customers, and other guests. Businesses are seeking better ways to:

- Provide secure wireless Internet access to visiting customers
- Enable limited access to company network resources for business partners
- Provide rapid authentication and connectivity for employees who are using their personal mobile devices

A Cisco Small Business wireless access point (AP), such as the WAP321 or WAP561, can be easily integrated into the existing wired network to provide a wireless connectivity with speed and security rivaling a typical wired connection.

The Cisco Captive Portal feature provides a convenient, secure, cost-effective way to offer wireless access for clients and other visitors while maintaining the security of your internal network. A guest network can serve many important business purposes, including streamlining business with partners and providing enhanced customer satisfaction and improve employee productivity

Captive Portal can provide the following basic functionality:

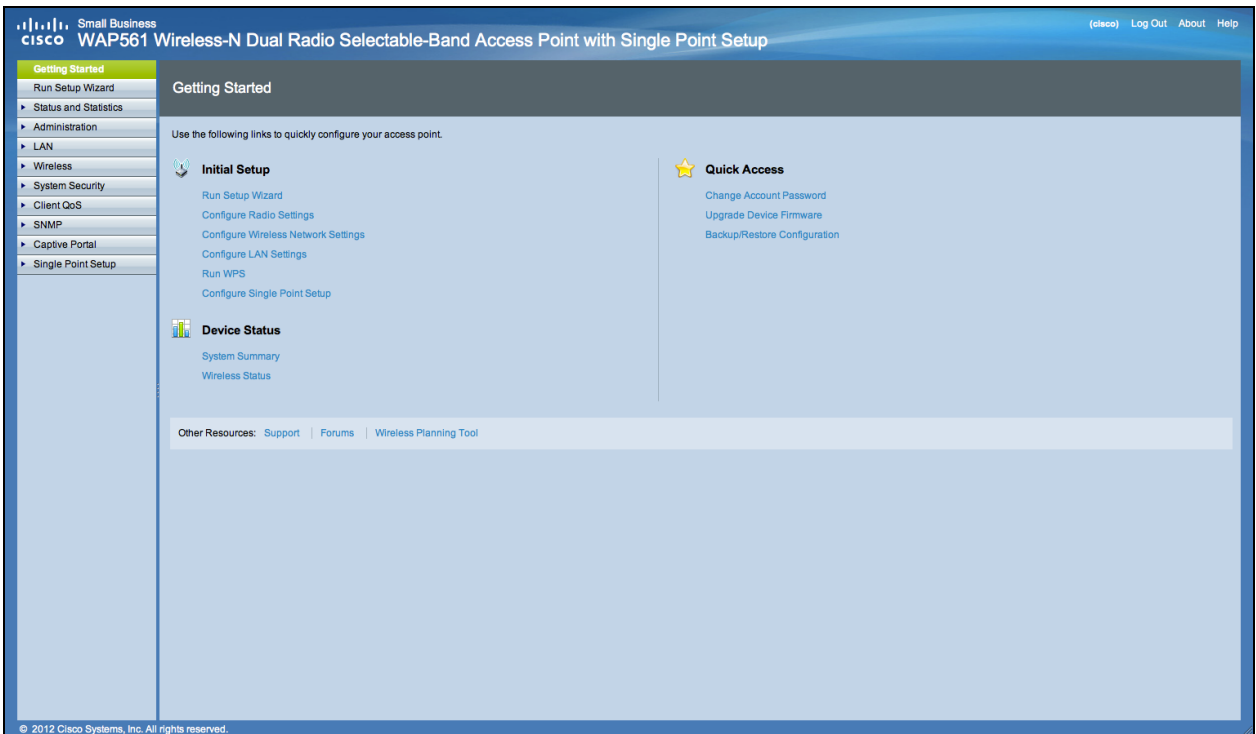
- Customized guest login page with company logos
- Ability to create multiple instances of the captive portal
- Multiple authentication options
- Ability to assign different rights and roles
- Ability to assign bandwidth (upstream and downstream)

## **How to Setup Captive Portal?**

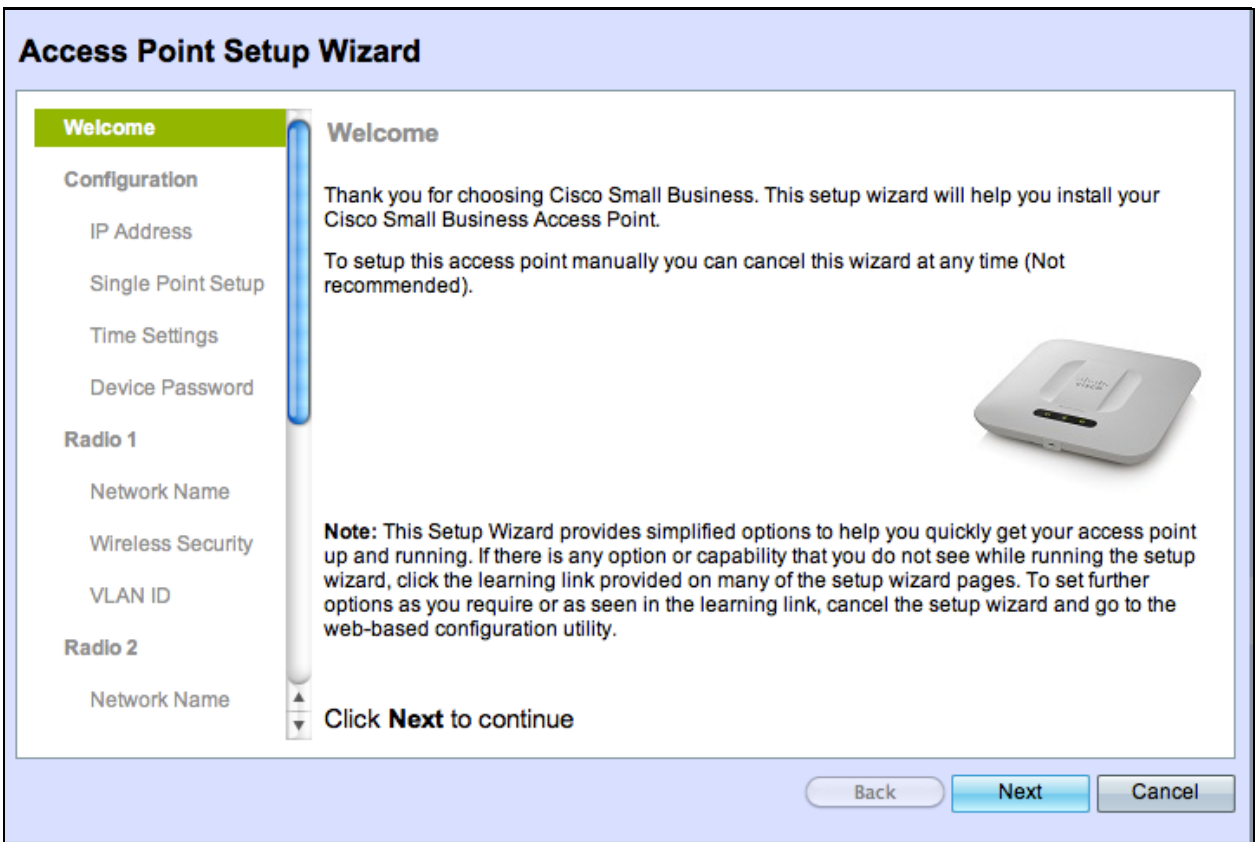
Captive Portal can be setup via the device GUI, for fast and basic setup customer can use the setup wizard to enable the feature, please see steps below:

### **Using the Setup Wizard**

Run the setup wizard from the main dashboard of the device GUI



Follow the wizard screens



Enable Guest access (Captive Portal)

### Access Point Setup Wizard

**Radio 2**

- ✓ Network Name
- ✓ Wireless Security
- ✓ VLAN ID

**Captive Portal**

- Creation
- Network Name
- Wireless Security
- VLAN ID
- Redirect URL
- Summary
- Finish

#### Enable Captive Portal - Create Your Guest Network

Use Captive Portal to set up a guest network, which means that wireless users need to be authenticated before they can access the Internet. For example, a hotel can create a guest network to redirect new wireless users to a page for authentication.

Do you want to create your guest network now?

Yes  
 No, thanks.

[? Learn more about captive portal guest networks](#)

Click **Next** to continue

Give your guest network a name, for example "My Company- Guest"

### Access Point Setup Wizard

**Radio 2**

- ✓ Network Name
- ✓ Wireless Security
- ✓ VLAN ID

**Captive Portal**

- ✓ Creation
- Network Name
- Wireless Security
- VLAN ID
- Redirect URL

Summary

Finish

#### Enable Captive Portal - Name Your Guest Network

Your guest network needs a new name, known as an SSID. The name identifies your guest network so that wireless users can find it.

Enter a name for your guest network:

Radio:  Radio 1  
 Radio 2

Guest Network name:  For example: MyGuestNetwork

[? Learn more about network names](#)

Click **Next** to continue

Select a security type.

### Access Point Setup Wizard

**Radio 2**

- ✓ Network Name
- ✓ Wireless Security
- ✓ VLAN ID

**Captive Portal**

- ✓ Creation
- ✓ Network Name
- Wireless Security
- VLAN ID
- Redirect URL

Summary

Finish

#### Enable Captive Portal - Secure Your Guest Network

Select your guest network security strength.

Best Security (WPA2 Personal - AES)  
Recommended for new wireless computers and devices that support this option. Older wireless devices might not support this option.

Better Security (WPA Personal - TKIP/AES)  
Recommended for older wireless computers and devices that might not support WPA2.

No Security (Not recommended)

Enter a security key with 8-63 characters.

Below Minimum

Show Key as Clear Text

[? Learn more about your network security options](#)

Click **Next** to continue

### Access Point Setup Wizard

**Radio 2**

- ✓ Network Name
- ✓ Wireless Security
- ✓ VLAN ID

**Captive Portal**

- ✓ Creation
- ✓ Network Name
- ✓ Wireless Security

**VLAN ID**

Redirect URL

Summary

Finish

#### Enable Captive Portal - Assign The VLAN ID

We strongly recommend that you assign different VLAN ID for your guest network than the management VLAN ID. By doing that, your guest will have no access to your private network.

Enter a VLAN ID for your guest network:

VLAN ID:  (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Back Next Cancel

If you have a specific web page you want to show after users accept the terms of service from the welcome page, type in the URL and then next, this URL can be your company website

### Access Point Setup Wizard

- ✓ Device Password
- ✓ Network Name
- ✓ Wireless Security
- ✓ VLAN ID
- Captive Portal**
  - ✓ Creation
  - ✓ Network Name
  - ✓ Wireless Security
  - ✓ VLAN ID
  - Redirect URL**
  - Summary
  - Finish

#### Enable Captive Portal - Enable Redirect URL

If you enable a redirect URL, when new wireless users have completed the authentication process, they can be redirected to an alternate startup page.

Enable Redirect URL

Redirect URL :

[? Learn more about redirect urls](#)

Click **Next** to continue

### Access Point Setup Wizard

- ✓ Device Password
- ✓ Network Name
- ✓ Wireless Security
- ✓ VLAN ID
- Captive Portal**
  - ✓ Creation
  - ✓ Network Name
  - ✓ Wireless Security
  - ✓ VLAN ID
  - ✓ Redirect URL
  - Summary**
  - Finish

#### Summary - Confirm Your Settings

Please review the following settings and ensure the data is correct.

Network Name (SSID):	ciscosb
Network Security Type:	plain-text
Security Key:	
VLAN ID:	1

Captive Portal (Guest Network) Summary

Network Name (SSID):	WAP321-guest
Network Security Type:	WPA2 Personal - AES
Security Key:	cisco,123
Verification:	Guest
Redirect URL:	N/A
VLAN ID:	1

Note: The AP Radio will be enabled after clicking Submit.

Click **Submit** to enable settings on your Cisco Small Business Access Point

Select Next to go to the next page

### Access Point Setup Wizard

**Radio 2**

- ✓ Network Name
- ✓ Wireless Security
- ✓ VLAN ID

**Captive Portal**

- ✓ Creation
- ✓ Network Name
- ✓ Wireless Security
- ✓ VLAN ID
- ✓ Redirect URL

**Summary**

- Finish


#### Device Setup Complete

✓ Congratulations, your access point has been set up successfully. We strongly recommend that you save these settings by writing them down or by copying and pasting them into a text document. You will need these settings later when you add other wireless computers or devices to your network.

Cluster Name:	ciscosb-cluster
Network Name (SSID):	ciscosb
Network Security Type:	plain-text
Security Key:	

Note: To configure WPS, Click "Run WPS" on the Getting Started page, under Initial Setup.

Click **Finish** to close this wizard.

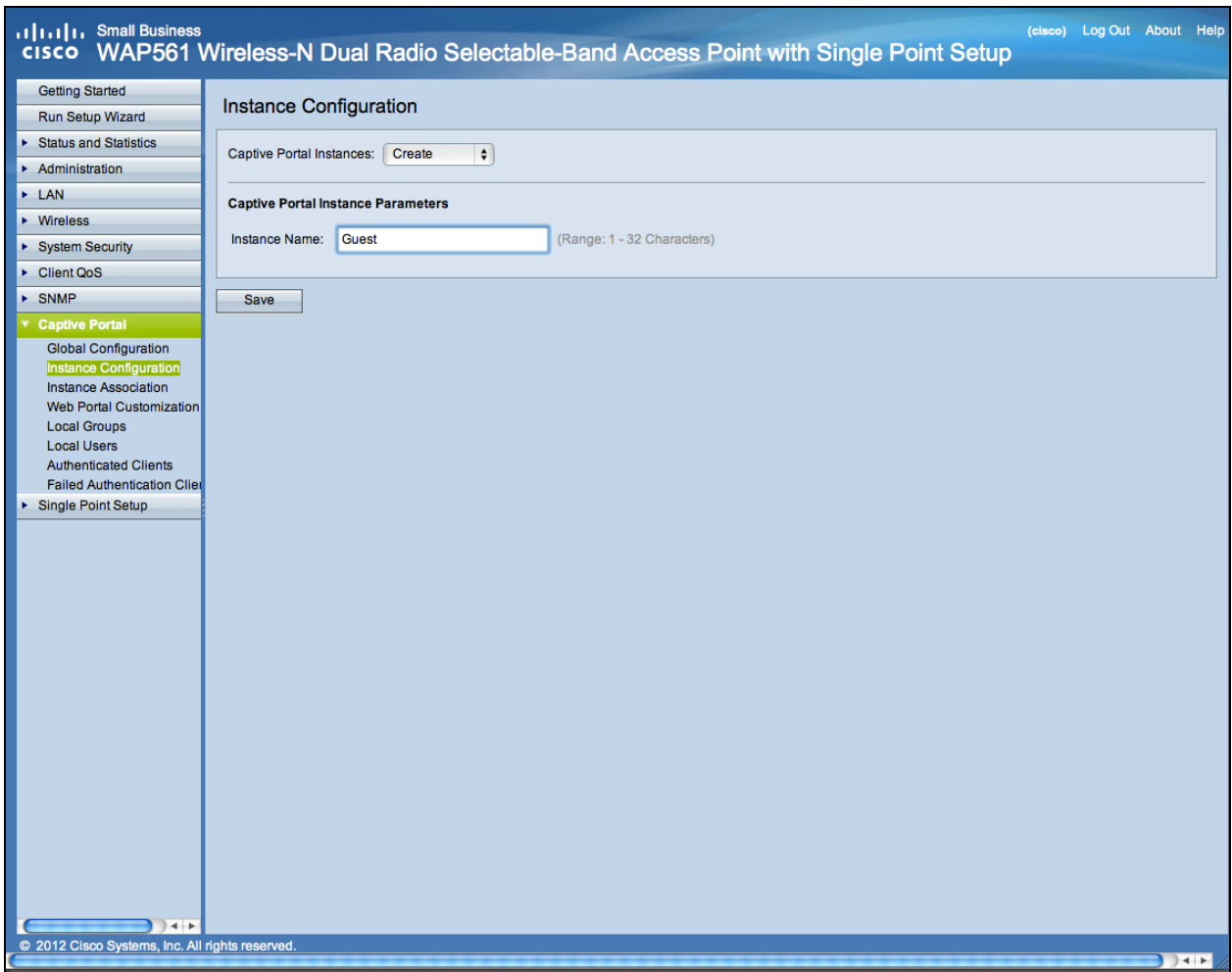


Back
Finish
Cancel

Now your Captive Portal setup is complete, now your customer is able to connect to your guest network and get the welcome page

For advance Setup and customization of the portal, please login to the Device GUI, from the Captive Portal menu

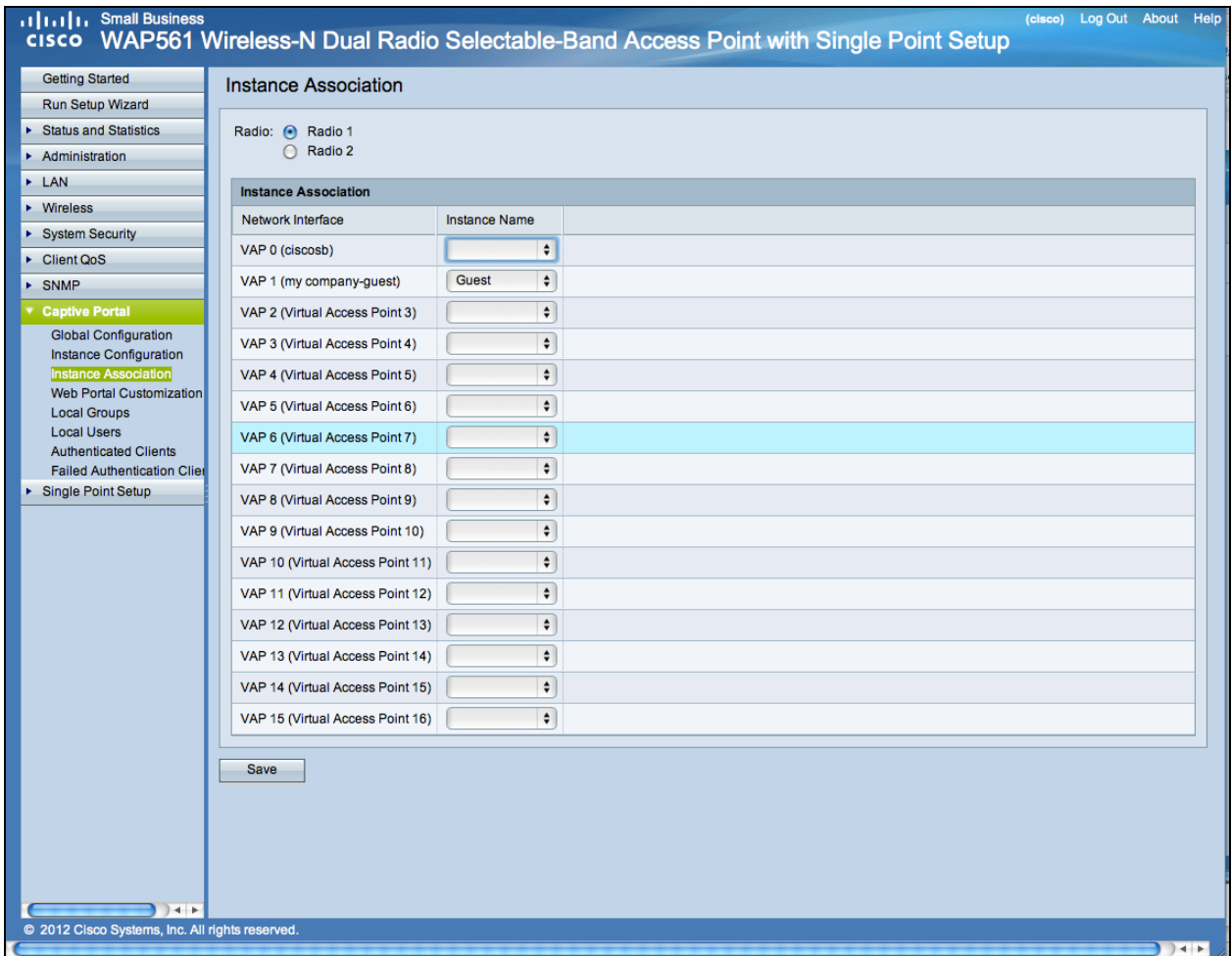
Select Instance Configuration, you will notice the wizard created an Instance name called "wiz-cp-inst1" you can choose this name or create a new name for your Instance Configuration and then save. If you choose the "wiz-cp-inst1" the screen will take you to the Instance Configuration page



You will notice that the setup wizard automatically associated captive portal instance name "**wiz-cp-inst1**" to the Guest SSID you're created during the setup wizard

If you created the instance using the GUI, now you need to associate to the guest network you created  
 From dropdown menu select the Instance Name "Guest", or the instance that was created by the wizard "**wiz-cp-inst1**"

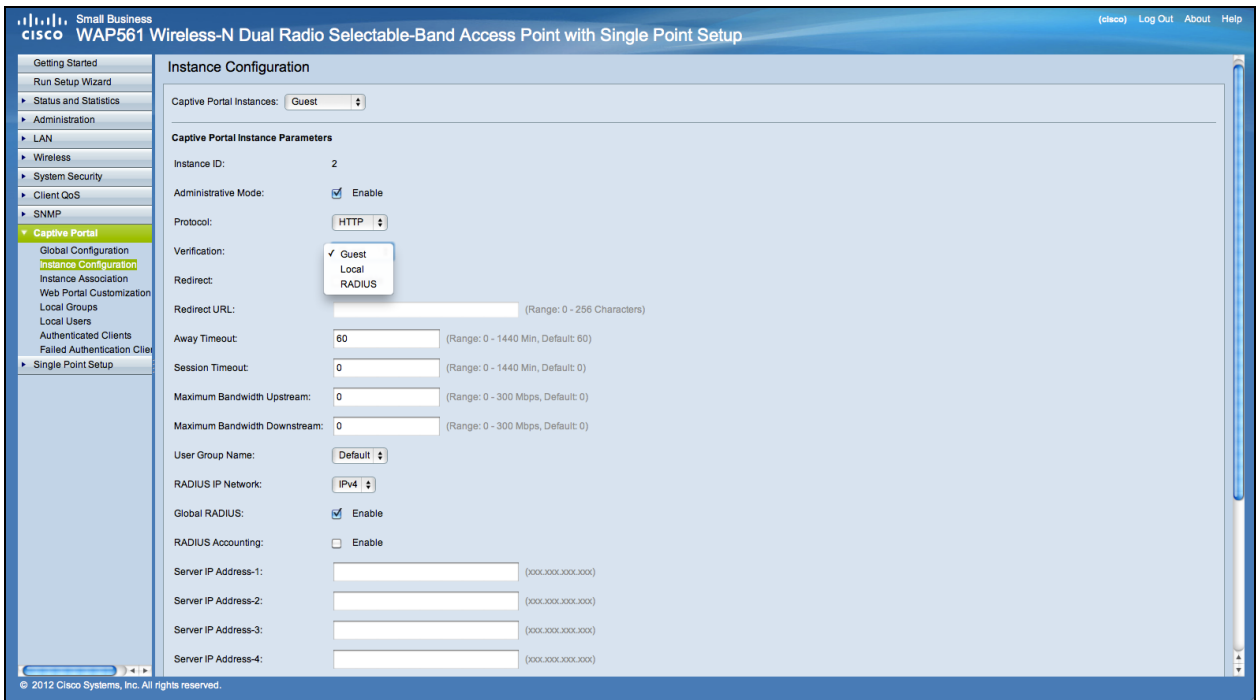




From the menu select Web Portal Configuration to configure your guest welcome page, choose the instance name from the drop down menu.

Select the authentication method for Captive Portal to use to verify clients:

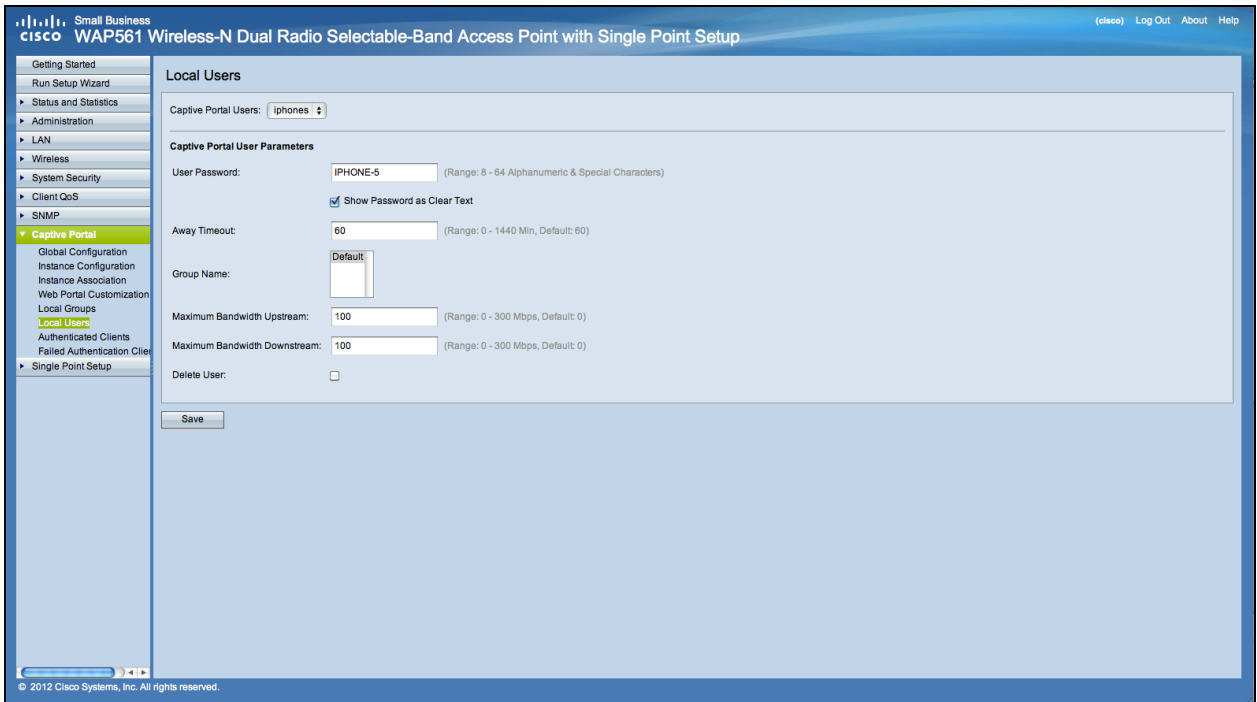
- Guest — The user does not need to be authenticated by a database.
- Local — The WAP device uses a local database to authenticated users.
- RADIUS — The WAP device uses a database on a remote RADIUS server to authenticate users.



If you choose verification method "Locale" then you need to create local users

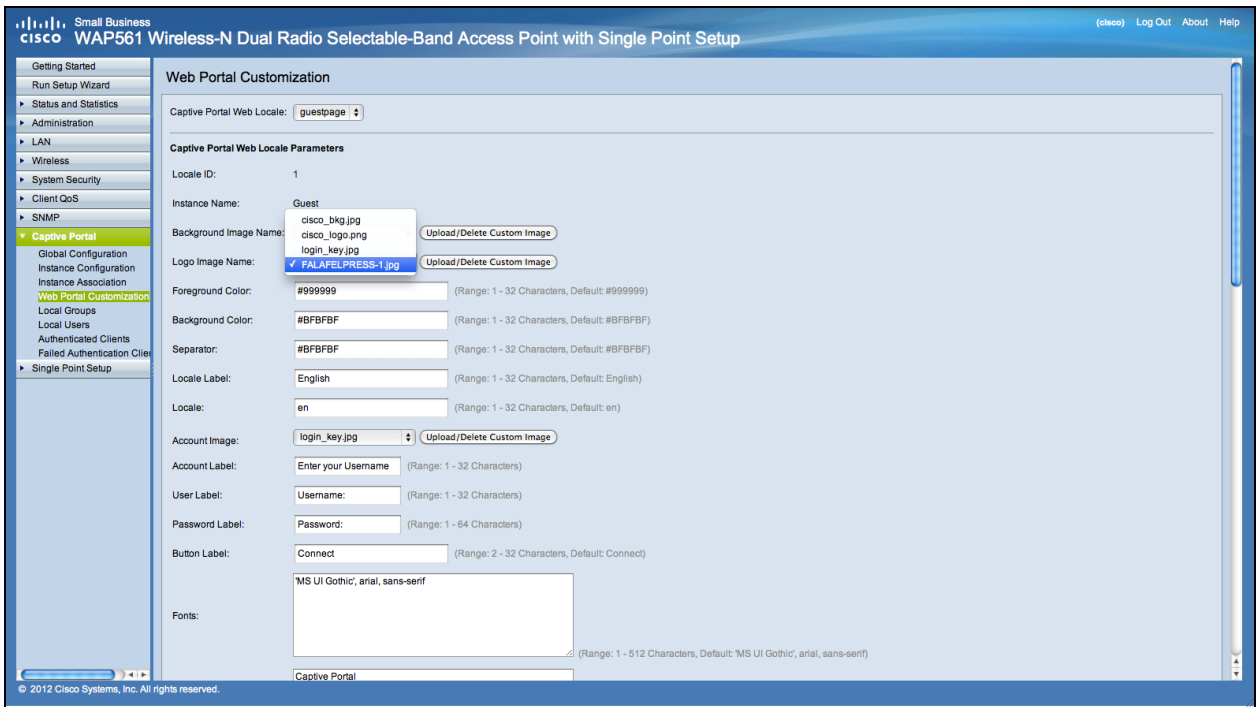
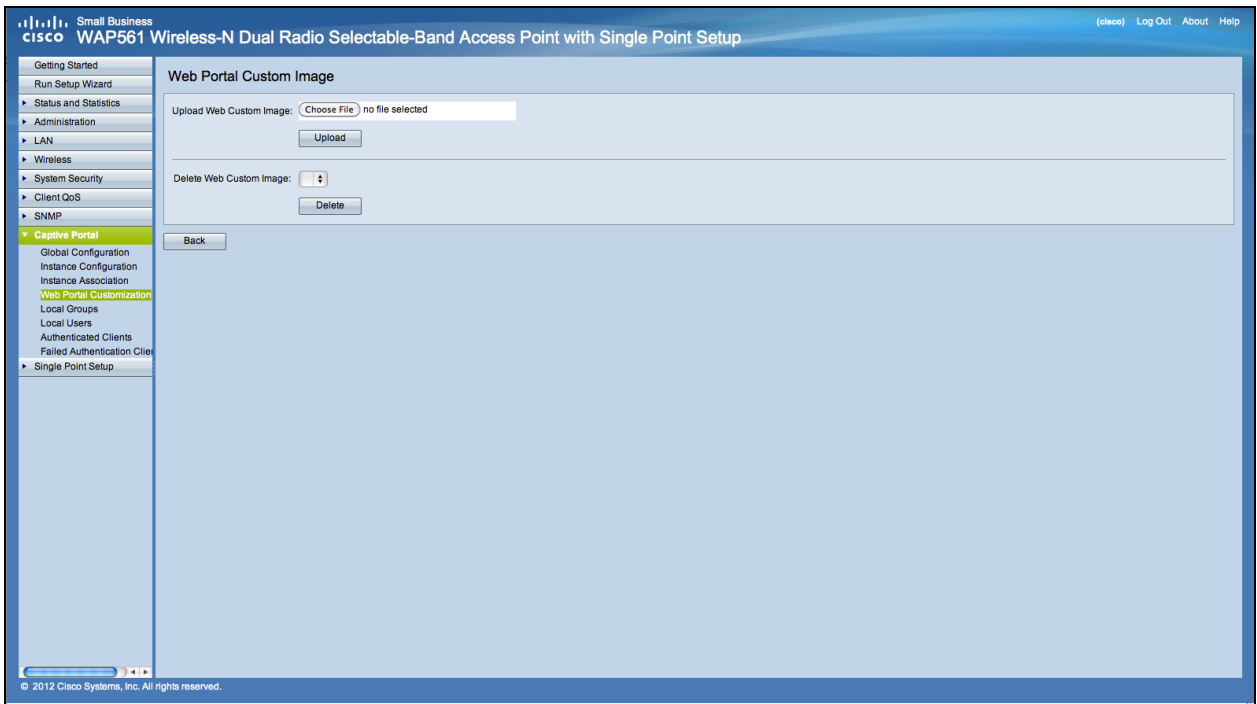
From the menu choose Local,

Enter the use parameter (name of the user), choose the parameters for the user profile.



Web Portal Page Customization, now you have the choice to upload your company logo and graphics you can upload up to 3 graphic files, one for the page background (Default cisco-bkg) second for the company logo (default, cisco-log) and third for the login screen (default, log-key)

\*\* Please note the file size for this artwork file need to be 5KB

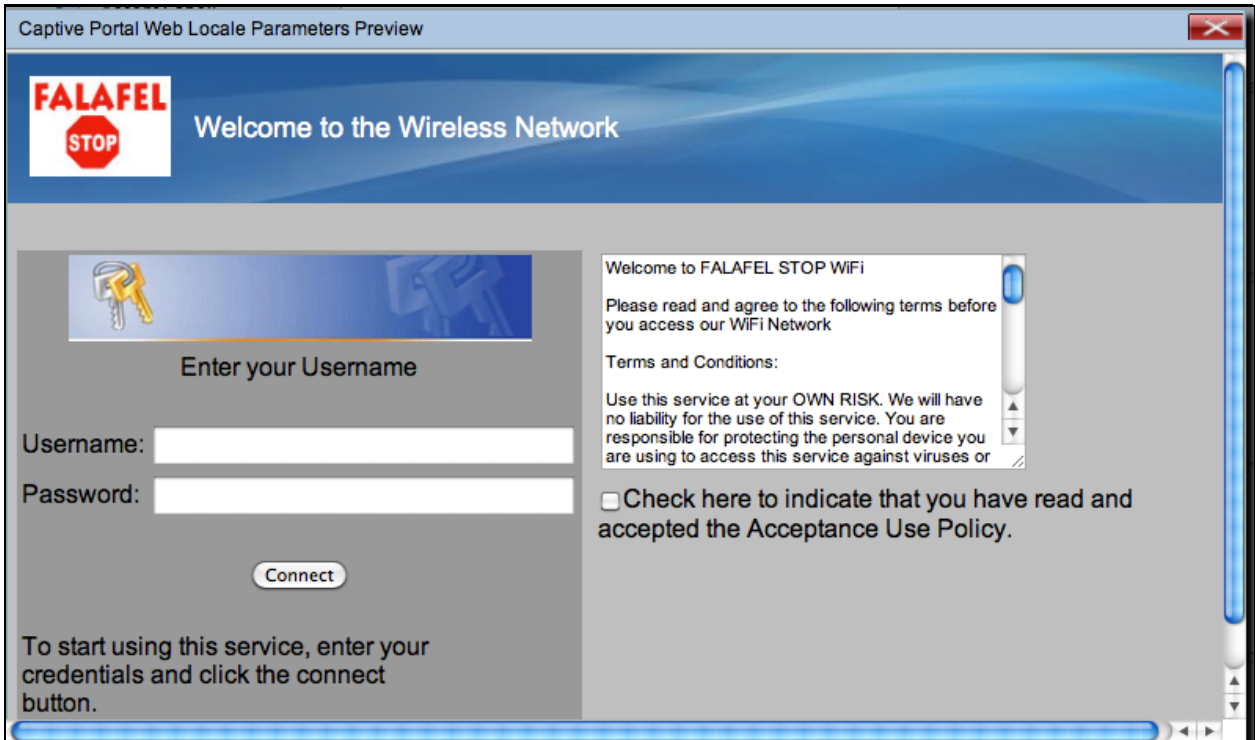


Now you can customize your web portal page, like add Acceptance Use Policy, window title and name and so on...

Customized page with verification method as Guest, this means no need to authenticate, user will only need to accept the terms of service and select the Connect button, entering the user name is optional



Customized page with verification method as Local this means user need to enter there user name and password to authenticate, and then user will need to accept the terms of service and select the Connect button



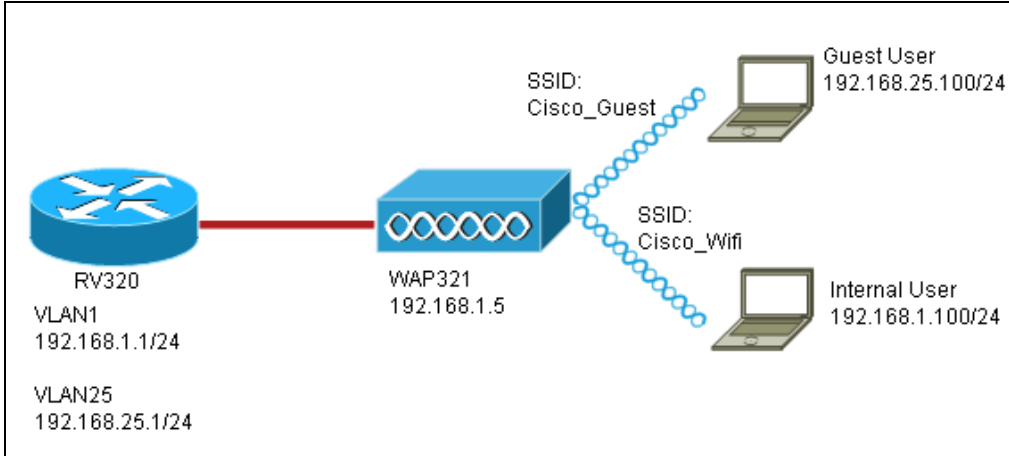
## Captive Portal in a Multi-VLAN Environment

In some cases a network has need of multiple VLANs for different purposes, servicing different groups of users. A common example is a separate network for Guest Users to prevent unauthorized users from accessing resources on the corporate network. Sometimes there are multiple wireless networks that need to be available to different users for the same reason. The WAP321 and

WAP561 can meet these needs using the Captive Portal, but do require a bit of additional configuration on the network. This section will go over that configuration.

**Intro – Existing configuration**

This document assumes that a network configuration is already in place. In this example, there are two networks, the main network and the guest network. The configuration to create and serve DHCP addresses to each network has already been configured. The WAP321 has already been configured to broadcast a different SSID for each network. The current setup will look like this:



When the configuration is complete, InterVLAN routing will be enabled on the network so that all wireless clients can access the Captive Portal, enabling network connectivity.

**Configuration**

First, enable interVLAN routing on the core router, in this case a RV320. To configure this go to Port Management > VLAN Membership to enable InterVLAN routing. Check both VLAN 1 and 25 on the left of the page and click Edit. In the InterVLAN Routing column, click on the dropdown box for each and select Enabled. Save the settings.

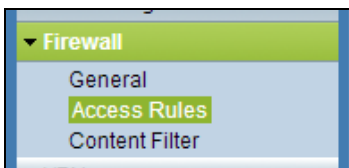
**VLAN Membership**

VLAN:  Enable  
 Create VLANs and assign the Outgoing Frame Type.  
 Up to four new VLANs can be created. VLAN IDs must be in the range (4..4094)

VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4
<input type="checkbox"/> 1	Default	Enabled	Enabled	Untagged	Untagged	Untagged	Untagged
<input type="checkbox"/> 25	Guest	Enabled	Disabled	Tagged	Tagged	Tagged	Tagged
<input type="checkbox"/> 100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged

Buttons: Add, Edit, Delete, Save, Cancel

Now all users should be able to access the captive portal, but they can also access any resources on either the main VLAN or the Guest VLAN. To restrict access, configure an access control rule on the RV320. Go to Firewall > Access Rules in order to configure this restriction.



At the bottom of the page, click Add. We want to add a total of 2 access rules for our scenario. First, configure the rule denying

access from the 192.168.25.x/24 guest subnet to the 192.168.1.x/24 internal subnet, as displayed to the right.

### Edit Access Rules

**Services**

Action:

Service:

Log:

Source Interface:

Source IP:   To

Destination IP:   To

---

**Scheduling**

Time:

From:  (hh:mm)

To:  (hh:mm)

Effective on:  Everyday  Sun  Mon  Tue  Wed  Thu  Fri  Sat

Click Save at the bottom of the page, then click back. Now add another rule, this time set the action as "Allow" and the destination IP as "Single." Configure the rule to allow access from the 192.168.25.x/24 subnet to 192.168.1.5, which is currently configured to be the WAP321 static IP. This rule will be placed ahead of the deny rule we just created, allowing traffic to 192.168.1.5 from the guest network and nowhere else on the main network.

When you are finished the access rules page should look like this.

### Access Rules

IPv4  IPv6

Access Rules Table								Items
	Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time
<input type="radio"/>	1	<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	192.168.25.1 ~ 192.168.25.254	192.168.1.5 ~ 192.168.1.5	Always
<input type="radio"/>	2	<input checked="" type="checkbox"/>	Deny	All Traffic [1]	LAN	192.168.25.1 ~ 192.168.25.254	192.168.1.1 ~ 192.168.1.254	Always
<input type="radio"/>		<input checked="" type="checkbox"/>	Allow	All Traffic [1]	LAN	Any	Any	Always
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB1	Any	Any	Always
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	USB2	Any	Any	Always
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN1	Any	Any	Always
<input type="radio"/>		<input checked="" type="checkbox"/>	Deny	All Traffic [1]	WAN2	Any	Any	Always

To configure captive portal in this setup, simply follow the steps from the first section for each network you need to configure the captive portal.

© 2013 Cisco Systems, Inc. All rights reserved.