

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 there 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

Enable a Captive Portal on your Cisco Wireless Network

cisco WAP561	ss Wireless-N Dual Radio Selectable-Band Access Point with Single Point Setup				
Getting Started Run Setup Wizard Status and Statistics	Getting Started				
Administration LAN	Use the following links to quickly configure your access point.				
Virreless System Security Glient QoS SNMP Captive Portal Single Point Setup	Initial Setup Initial Setup Run Setup Wizard Change Account Password Configure Radio Settings Upgrade Device Firmware Configure UAN Settings BackupRestore Configuration Configure Single Point Setup BackupRestore Configuration Image Room Summary Wreless Status Device Status				
	Other Resources: Support Forums Wreless Planning Tool				

Follow the wizard screens

ccess Point Setu	p Wizard
Welcome	Welcome
Configuration	Thank you for choosing Cisco Small Business. This setup wizard will help you install your Cisco Small Business Access Point
IP Address	Cisco Sinaii Business Access Folini.
Single Point Setup	To setup this access point manually you can cancel this wizard at any time (Not recommended).
Time Settings	
Device Password	Jame D
Radio 1	
Network Name	
Wireless Security	Note: This Setup Wizard provides simplified options to help you quickly get your access point up and running. If there is any option or capability that you do not see while running the setup
VLAN ID	wizard, click the learning link provided on many of the setup wizard pages. To set further options as you require or as seen in the learning link, cancel the setup wizard and go to the
Radio 2	web-based configuration utility.
Network Name	Click Next to continue
	Back Next Cancel

Enable Guest access (Captive Portal)



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

Access Point Setu	ıp Wizard	
Radio 2	Enable Captive	Portal - Name Your Guest Network
 Network Name 	Your guest network	needs a new name, known as an SSID. The name identifies your quest
✓ Wireless Security	network so that wire	less users can find it.
VLAN ID	Enter a name for you	ur guest network:
Captive Portal	Radio:	Radio 1
✓ Creation		Radio 2
Network Name	Guest Network name	e: My Company- Guest
Wireless Security		For example: MyGuestNetwork
VLAN ID		
Redirect URL	Learn more abou	t network names
Summary		
Finish	Click Next to cor	ntinue
		Back Next Cancel



Radio 2	Enable Captive Portal - Secure Your Guest Network
 Network Name 	Select your quest network security
 Wireless Security 	strength.
VLAN ID	Best Security (WPA2 Personal - AES) Recommended for new wireless computers and devices that support this option. Older wireless devices might not support this option.
Captive Portal	Better Security (WPA Personal - TKIP/AES)
Creation	Recommended for older wireless computers and devices that might not support WPA2.
✓ Network Name	No Security (Not recommended)
Wireless Security	
VLAN ID	characters.
Redirect URL	Below Minimum
Summary	Show Key as Clear Text
Finish	QLearn more about your network security options
1 mon	Click Next to continue

Access Point Setup Wizard						
Radio 2	Enable Captive Portal - Assign The VLAN ID					
 Network Name 	We strongly recommend that you assign different VLAN ID for your quest network than the					
 Wireless Security 	management VLAN ID. By doing that, your guest will have no access to your private network.					
VLAN ID	Enter a VLAN ID for your guest network:					
Captive Portal	VLAN ID: 1 (Range: 1 - 4094)					
 Creation 						
 Network Name 	Learn more about vian ids					
✓ Wireless Security						
VLAN ID						
Redirect URL						
Summary						
Finish	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 Setur	p Wizard
✓ Device Password	Enable Captive Portal - Enable Redirect URL
 Network Name 	If you enable a redirect URL, when new wireless users have completed the authentication
✓ Wireless Security	process, they can be redirected to an alternate startup page.
VLAN ID	Enable Redirect URL
Captive Portal	Redirect URL :
✓ Creation	2 Learn more about redirect urls
Network Name	
✓ Wireless Security	
VLAN ID	
Redirect URL	
Summary	
Finish	Click Next to continue
	Back Next Cancel



Select Next to go to the next page

Access Point Setu	p Wizard
Radio 2	Device Setup Complete
 ✓ Network Name ✓ Wireless Security ✓ VLAN ID 	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.
Captive Portal	
 Creation 	Cluster Name: ciscosb-cluster
 Network Name 	Network Name (SSID): ciscosb Network Security Type: plain-text
 Wireless Security 	Security Key:
 ✓ VLAN ID ✓ Redirect URL 	Note: To configure WPS, Click "Run WPS" on the Getting Started page, under Initial Setup.
Summary	
Finish	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

ı ۱۱۱۱، Small Business cısco WAP561 V	(disco) Log Out About Help Wireless-N Dual Radio Selectable-Band Access Point with Single Point Setup
Getting Started	lastana Carlinustian
Run Setup Wizard	Instance Configuration
 Status and Statistics 	Cantive Portal Instances: Create
 Administration 	
► LAN	Captive Portal Instance Parameters
 Wireless 	
 System Security 	Instance Name: Guest (Range: 1 - 32 Characters)
 Client QoS 	
► SNMP	Save
Captive Portal	
Global Configuration Instance Configuration Instance Association Web Portal Customization	
Local Groups	
Local Users	
Failed Authentication Clier	
 Single Point Setup 	
© 2012 Cisco Systems, Inc. All	rights reserved.

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 setupwizard

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"

Run Setup Wizard							
Status and Statistics							
	Radio: 💿 Radio 1						
 Administration 	Radio 2						
► LAN	Instance Association						
 Wireless 	Network Interface Instance Name						
 System Security 	VAP 0 (ciscosh)						
 Client QoS 			-				-
SNMP	VAP 1 (my company-guest)	Guest	•				
Captive Portal	VAP 2 (Virtual Access Point 3)		\$				
Global Configuration	VAP 3 (Virtual Access Point 4)		\$				
Instance Association	VAP 4 (Virtual Access Point 5)		•				
Web Portal Customization Local Groups	VAP 5 (Virtual Access Point 6)		•				
Local Users	VAP 6 (Virtual Access Point 7)		•				
Failed Authentication Clier	VAP 7 (Virtual Access Point 8)		\$				
 Single Point Setup 	VAP 8 (Virtual Access Point 9)		•				
	VAP 9 (Virtual Access Point 10)		\$				
	VAP 10 (Virtual Access Point 11)		\$				
	VAP 11 (Virtual Access Point 12)		\$				
	VAP 12 (Virtual Access Point 13)		•				
	VAP 13 (Virtual Access Point 14)		•				
	VAP 14 (Virtual Access Point 15)		•				
	VAP 15 (Virtual Access Point 16)		\$				

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.

cisco WAP561 V	Wireless-N Dual Radio Selectable-Band Access Point with Single Point Setup	(cisco) Log Out About Hel
Getting Started	Instance Configuration	
Run Setup Wizard		
 Status and Statistics 	Captive Portal Instances: Guest 🗘	
 Administration 		
► LAN	Captive Portal Instance Parameters	
 Wireless 	Instance ID: 2	
System Security	Administrative Meder CE Enable	
Client Qos		
Captive Portal	Protocol:	
Global Configuration	Verification: Vegest	
Instance Configuration	Redirect	
Web Portal Customization	RADIUS	
Local Groups	Redirect URL: (Range: 0 - 256 Characters)	
Authenticated Clients	Away Timeout 60 (Range: 0 - 1440 Min, Default: 60)	
Failed Authentication Clier		
· Single Fornt Setup	Session Timeout: U (Range: 0 - 1440 Min, Detault: 0)	
	Maximum Bandwidth Upstream: 0 (Range: 0 - 300 Mbps, Default: 0)	
	Maximum Bandwidth Downstream: 0 (Range: 0 - 300 Mbps, Default: 0)	
	User Group Name: Default 🗘	
	RADIUS IP Network:	
	Global RADIUS: 🗹 Enable	
	RADIUS Accounting: Enable	
	Server IP Address-1: (0000000000000)	
	Server IP Address-2: (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	
	Server IP Address-3: (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	
	Server IP Address-4: (xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	
© 2012 Cisco Systems, Inc. All	inghis reserved.	

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.

cisco WAP561	Wireless-N Dual Radio	Selectable-Bar	nd Access Point with Single Point Setup	(cisco) L	og Out 🖌	About H	Help	
Getting Started Run Setup Wizard	Local Users							
Status and Statistics Administration	Captive Portal Users: iphones \$	aplive Portal Users: phones \$						
LAN Mirologg	Captive Portal User Parameters	Captive Portal User Parameters						
System Security	User Password:	IPHONE-5	(Range: 8 - 64 Alphanumeric & Special Characters)					
Client QoS SNMP		Show Password as Cl	ear Text					
Captive Portal Global Configuration	Away Timeout:	60	(Range: 0 - 1440 Min, Default: 60)					
Instance Configuration Instance Association Web Portal Customization	Group Name:	Default						
Local Groups Local Users	Maximum Bandwidth Upstream:	100	(Range: 0 - 300 Mbps, Default: 0)					
Failed Authentication Client	Maximum Bandwidth Downstream:	100	(Range: 0 - 300 Mbps, Default: 0)					
· ongie i on oetap	Delete User:							
	Save							
© 2012 Cisco Systems, Inc. All	rights reserved.							

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

cisco WAP561	Vireless-N Dual Radio Selectable-Band Access Point with Single Point Setup	(cisco)	Log Out	About	Help
Getting Started Run Setup Wizard	Web Portal Custom Image				
Status and Statistics Administration	Upload Web Custom Image: Choose File no file selected				
Vireless System Security	Delete Web Custom Image:				-
Client QoS SNMP	Delete				
Captor Portal Global Configuration Instance Association Mveb Fordi Centiguration Local Groups Local Users Authenticated Clinits Failed Authentication Cliev Single Point Setup	Back				
2012 Cisco Systems, Inc. Ali	richts meerved.				
S 2012 Claco Systems, Inc. All	ngina readition.				

cisco WAP561	Vireless-N Dual F	Radio Selectable-Band Access Point with Single Point Setup	(cisco)		About	Help		
Getting Started Run Setup Wizard	Web Portal Custom	nization				n		
Status and Statistics Administration	Captive Portal Web Locale:	: guespage 🕽						
► LAN	Captive Portal Web Locale	Capitive Portal Web Locale Parameters						
System Security	Locale ID:	1						
 SNMP 	Instance Name:	Guest cisco_bkg.jpg						
Captive Portal Global Configuration	Logo Image Name:	login key jog / FAI AFELPERSS-1 jog (Upload/Delete Custom image)						
Instance Association Web Portal Customization	Foreground Color:	#999999 (Range: 1 - 32 Characters, Default: #999999)				U		
Local Groups Local Users Authenticated Clients	Background Color:	#BFBFBF (Range: 1 - 32 Characters, Default: #BFBFBF)						
Failed Authentication Clier Single Point Setup	Separator:	#BFBFBF (Range: 1 - 32 Characters, Default: #BFBFBF)						
	Locale Label:	English (Range: 1 - 32 Characters, Default English)						
	Account Image:	login_keyjpg (Upload/Delete Custom Image)						
	Account Label:	Enter your Usemame (Range: 1 - 32 Characters)						
	User Label:	Username: (Range: 1 - 32 Characters)						
	Password Label:	Password: (Range: 1 - 64 Characters)						
	Button Label:	Connect (Range: 2 - 32 Characters, Default Connect)						
	Fonts:							
		/ (Rance: 1 - 512 Characters, Default, %S UI Gothic, arial, sans-senfi						
© 2012 Cisco Systems, Inc. All	rights reserved.	Captive Portal				À T		
						<u> </u>		

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

Captive Portal Web Locale Parameters Preview							
Welcome to the Wireless Netwo	ork						
Enter your Username Username: Connect To start using this service, enter your credentials and click the connect button.	Welcome to FALAFEL STOP WiFi Please read and agree to the following terms before you access our WiFi Network Terms and Conditions: Use this service at your OWN RISK. We will have no liability for the use of this service. You are responsible for protecting the personal device you are using to access this service against viruses or Check here to indicate that you have read and accepted the Acceptance Use Policy.						

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 Web Locale Parameters Preview					
Welcome to the Wireless Netwo	ork				
Enter your Username Username: Password: Connect To start using this service, enter your credentials and click the connect button.	Welcome to FALAFEL STOP WiFi Please read and agree to the following terms before you access our WiFi Network Terms and Conditions: Use this service at your OWN RISK. We will have no liability for the use of this service. You are responsible for protecting the personal device you are using to access this service against viruses or Check here to indicate that you have read and accepted the Acceptance Use Policy.				

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.

٧	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 (44094)										
	VLAN Table Items 1-3 of 3 5										
		VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2	LAN3	LAN4		
		1	Default	Enabled 💌	Enabled	Untagged 💌	Untagged 💌	Untagged 💌	Untagged 💌		
		25	Guest	Enabled 💌	Disabled 💌	Tagged 💌	Tagged 💌	Tagged 💌	Tagged 💌		
		100	Voice	Disabled	Disabled	Tagged	Tagged	Tagged	Tagged		
	Add Edit Delete Page 1 v of 1										
	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:	Deny 🗸						
Service:	All Traffic [TCP&UDP/1~65535]						
Log:	No Log						
Source Interface:	LAN						
Source IP:	Range 🗨 192.168.25.1 To 192.168.25.254						
Destination IP:	Range 192.168.1.1 To 192.168.1.254						
Scheduling							
Time:	Always 💌						
From:	(hh:mm)						
To:	(hh:mm)						
Effective on:	V Everyday Sun Mon Tue Wed Thu Fri Sat						
Save Cancel Back							

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.

A	Access Rules										
1	Pv4	IPv6									
	Acce	ess Rules Tab	ole						Items		
		Priority	Enable	Action	Service	SourceInterface	Source	Destination	Time		
	\odot	1 💌		Allow	All Traffic [1]	LAN	192.168.25.1 ~ 192.168.25.254	192.168.1.5 ~ 192.168.1.5	Always		
	\bigcirc	2 💌		Deny	All Traffic [1]	LAN	192.168.25.1 ~ 192.168.25.254	192.168.1.1 ~ 192.168.1.25	4 Always		
			\checkmark	Allow	All Traffic [1]	LAN	Any	Any	Always		
	0		\checkmark	Deny	All Traffic [1]	USB1	Any	Any	Always		
			\checkmark	Deny	All Traffic [1]	USB2	Any	Any	Always		
			\checkmark	Deny	All Traffic [1]	WAN1	Any	Any	Always		
			Image: A start of the start	Deny	All Traffic [1]	WAN2	Any	Any	Always		
	Add	Edit	Delete	Restore to Defa	ult Rules	Service Management			Page		

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.