

Configuration of Captive Portal on the RV130W

Objective

Captive portal turns a web browser into an authentication device. The web page requires user interaction or authentication in order to grant network access to the user. Captive portals are commonly used at Wi-Fi hotspots to regulate access to the network through a password and username system.

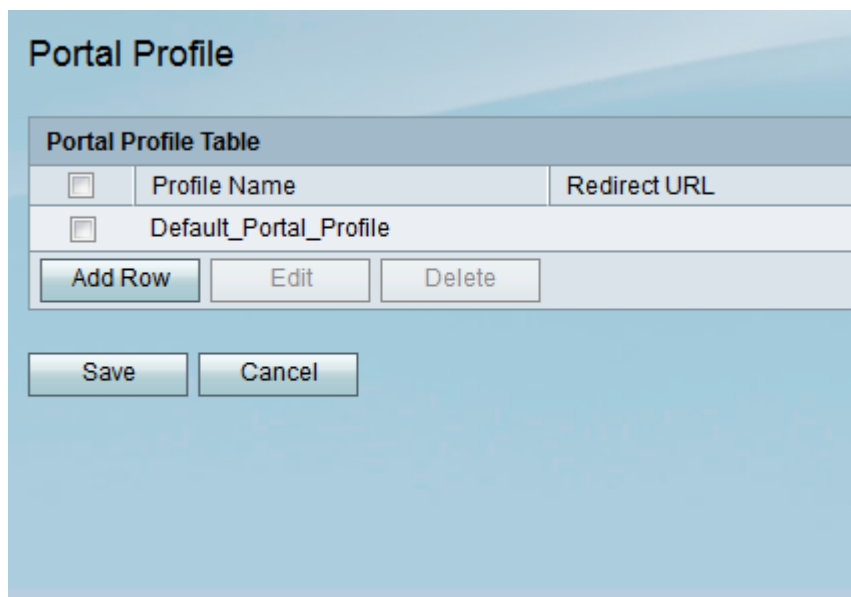
The objective of this document is to show you how to configure captive portal on the RV130W.

Applicable Devices

- RV130W

Add a Captive Portal Profile

Step 1. Log in to the web configuration utility and choose **Wireless > Captive Portal > Portal Profile**. The *Portal Profile* page opens:



The screenshot shows the 'Portal Profile' configuration page. At the top, there is a title 'Portal Profile'. Below it is a table with the following structure:

Portal Profile Table		
<input type="checkbox"/>	Profile Name	Redirect URL
<input type="checkbox"/>	Default_Portal_Profile	

Below the table are three buttons: 'Add Row', 'Edit', and 'Delete'. At the bottom of the page are two buttons: 'Save' and 'Cancel'.

Step 2. Click **Add Row** to add a new captive portal profile.

Portal Profile

Portal Profile Table	
<input type="checkbox"/>	Profile Name Redirect URL
<input type="checkbox"/>	Default_Portal_Profile
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

A new page of portal profile settings appears:

Portal Profile

Portal Profile Setting

Profile Name:

Verification:

Auto Redirect URL: Enable Disable

Redirect URL:

Session Timeout: Minutes (Range: 0 - 1440, Default: 0, Unlimited: 0)

Font Color:

Company Name:

Welcome Message:

Username Field:

Password Field:

Login Button Title:

Copyright:

Error 1:

Error 2:

Agreement: Enable Disable

Step 3. In the *Profile Name* field, enter a name for the captive portal profile.

Portal Profile Setting

Profile Name:

Verification:

Auto Redirect URL: Enable Disable

Redirect URL:

Session Timeout: Minutes (Range: 0 - 1440, Default: 0, Unlimited: 0)

Step 4. From the *Verification* drop-down list, select the method of authentication used to verify clients.

Portal Profile Setting

Profile Name:

Verification:

Auto Redirect URL: Local Disable

Redirect URL:

Session Timeout:

The available options are defined as follows:

- Guest — Client does not need to be authenticated by a database.
- Local — Device uses a local database to authenticate clients.

Step 5. In the *Auto Redirect URL* field, Click the **Enable** radio button to redirect clients to a specified web address when they log into the captive portal. If you do not want this feature, choose **Disable** and skip to Step 7.

Portal Profile

Portal Profile Setting

Profile Name:

Verification:

Auto Redirect URL: Enable Disable

Redirect URL:

Session Timeout:

Step 6. If you chose to enable Auto Redirect URL in Step 5, In the *Redirect URL* field, enter the address for the web page you would like client to be redirected to.

Portal Profile Setting

Profile Name:

Verification:

Auto Redirect URL: Enable Disable

Redirect URL:

Session Timeout:

Step 7. In the *Session Timeout* field, enter the time, in minutes, that a client is allowed to stay connected before they are logged out and re-authentication is required. Entering a value of **0** allows the client to stay connected for an unlimited time period.

Portal Profile Setting

Profile Name:

Verification:

Auto Redirect URL: Enable Disable

Redirect URL:

Session Timeout: Minutes (Range: 0 - 1440, Default: 0, Unlimited: 0)

Step 8. Choose a color for the text on the captive portal page from the *Font Color* drop-down list.

Font Color:

Company Name:

Welcome Message:

Username Field:

Password Field:

Login Button Title:

Step 9. In the *Company Name* field, enter the company name to be shown on the captive portal page.

Font Color:	White ▾
Company Name:	Small Business
Welcome Message:	Guest Access
Username Field:	Username
Password Field:	Password
Login Button Title:	Log In
Copyright:	© 2014 Cisco Systems Inc, All rights reserved.
Error 1:	Login failed. Incorrect username or password.
Error 2:	All Connections are currently in use, please try again a little later.

Step 10. In the *Welcome Message* field, enter the message that is shown when a client is successfully connected.

Font Color:	White ▾
Company Name:	Small Business
Welcome Message:	Guest Access
Username Field:	Username
Password Field:	Password
Login Button Title:	Log In
Copyright:	© 2014 Cisco Systems Inc, All rights reserved.
Error 1:	Login failed. Incorrect username or password.
Error 2:	All Connections are currently in use, please try again a little later.

Step 11. In the *Username* field and the *Password* field, Enter the text that is shown next to these fields when they are displayed on the captive portal page.

Font Color:	White ▾
Company Name:	Small Business
Welcome Message:	Guest Access
Username Field:	Username
Password Field:	Password
Login Button Title:	Log In
Copyright:	© 2014 Cisco Systems Inc, All rights reserved.
Error 1:	Login failed. Incorrect username or password.
Error 2:	All Connections are currently in use, please try again a little later.

Step 12. In the *Login Button Title* field, enter the text to be displayed on the login button of

the captive portal page.

Font Color:	White ▾
Company Name:	Small Business
Welcome Message:	Guest Access
Username Field:	Username
Password Field:	Password
Login Button Title:	Log In
Copyright:	© 2014 Cisco Systems Inc, All rights reserved.
Error 1:	Login failed. Incorrect username or password.
Error 2:	All Connections are currently in use, please try again a little later.

Step 13. In the *Copyright* field, enter a copyright to be shown at the bottom of the captive portal page.

Font Color:	White ▾
Company Name:	Small Business
Welcome Message:	Guest Access
Username Field:	Username
Password Field:	Password
Login Button Title:	Log In
Copyright:	© 2014 Cisco Systems Inc, All rights reserved.
Error 1:	Login failed. Incorrect username or password.
Error 2:	All Connections are currently in use, please try again a little later.

Step 14. Enter error messages to be shown in the *Error 1* and *Error 2* fields. Error 1 is for failed authentication due to invalid username or password. Error 2 is for when the network is busy and all connections are being used.

Font Color:	White
Company Name:	Small Business
Welcome Message:	Guest Access
Username Field:	Username
Password Field:	Password
Login Button Title:	Log In
Copyright:	© 2014 Cisco Systems Inc, All rights reserved.
Error 1:	Login failed. Incorrect username or password.
Error 2:	All Connections are currently in use, please try again a little later.

Step 15. In the *Agreement* field, Click the **Enable** radio button to require clients to read and agree to an acceptance policy prior to connecting. If you do not want this feature, choose **Disable** and skip to Step 18.

Error 1:	Login failed. Incorrect username or password.
Error 2:	All Connections are currently in use, please try again a little later.
Agreement:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Agreement Text:	Check here to indicate that you have read and accepted the Acceptance U
Acceptance Use Policy:	Acceptance the Policy.

Step 16. If you chose to enable an agreement policy in Step 15, enter the text in the *Agreement Text* field that will appear next to the agreement check box on the captive portal page.

Error 1:	Login failed. Incorrect username or password.
Error 2:	All Connections are currently in use, please try again a little later.
Agreement:	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Agreement Text:	Check here to indicate that you have read and accepted the Acceptance U
Acceptance Use Policy:	Acceptance the Policy.

Step 17. If you chose to enable an agreement policy in Step 15, enter in the *Acceptance Use Policy* field the text that will be displayed as the use policy on the captive portal page.

Error 1:

Error 2:

Agreement: Enable Disable

Agreement Text:

Acceptance Use Policy:


Step 18. If you wish to change the background image or logo that is displayed on the captive portal page, click **Browse** to select an image from your computer. When you are ready to add the item to the device, click **Upload** for the corresponding item.

Upload Files				
Item	Status	File Name	Select Image	
Background	Default		<input type="button" value="Browse..."/> No file selected. (*.jpg, Maximum size: 128 kbytes)	<input type="button" value="Upload"/>
Logo	Default		<input type="button" value="Browse..."/> No file selected. (*.gif, Maximum size: 10 kbytes)	<input type="button" value="Upload"/>

Step 19. Click **Save** to save your newly created captive portal profile.

Step 20. You will be redirected to the main *Portal Profile* page. Your new profile should be listed in the *Portal Profile Table*. Click **Save** to keep the profile saved onto your device.

Portal Profile

 Configuration settings have been saved successfully

Portal Profile Table		
<input type="checkbox"/>	Profile Name	Redirect URL
<input type="checkbox"/>	Default_Portal_Profile	
<input type="checkbox"/>	cisco1	https://www.cisco.com

Add User Accounts

User accounts with a username and password must exist for captive portal to function. Only clients with a user account stored in the device will be able to log in on the captive portal page and access the network.

Step 1. Navigate to **Wireless > Captive Portal > User Account** in the web configuration utility. The *User Account* page appears:

User Account

User Account Table		
<input type="checkbox"/>	Username	Password
<input type="checkbox"/>	No data to display	
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>
<input type="button" value="Save"/>		<input type="button" value="Cancel"/>

Step 2. Click **Add Row** to add a new user account to the *User Account Table*.

User Account

You must save before you can edit or delete.

User Account Table				
<input type="checkbox"/>	Username	Password	Verify Password	Access Time (Minutes)
<input type="checkbox"/>	user1	60
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Import"/>	
<input type="button" value="Save"/>		<input type="button" value="Cancel"/>		

Step 3. Enter a name for the user in the *Username* field.

User Account

You must save before you can edit or delete.

User Account Table				
<input type="checkbox"/>	Username	Password	Verify Password	Access Time (Minutes)
<input type="checkbox"/>	user1	60
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Import"/>	
<input type="button" value="Save"/>		<input type="button" value="Cancel"/>		

Step 4. Enter a password for the user account in the *Password* field. Enter the same password again in the *Verify Password* field.

User Account

You must save before you can edit or delete.

User Account Table				
<input type="checkbox"/>	Username	Password	Verify Password	Access Time (Minutes)
<input type="checkbox"/>	user1	60
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Import"/>	
<input type="button" value="Save"/>		<input type="button" value="Cancel"/>		

Step 5. Enter the time (in minutes) that the specific user will be allowed access to the network before needing to log in again in the *Access Time (Minutes)* field. Entering **0** will grant the user unlimited access.

User Account

You must save before you can edit or delete.

User Account Table

Username	Password	Verify Password	Access Time (Minutes)
user1	*****	*****	60

Add Row Edit Delete Import

Save Cancel

Step 6. Click **Save** to save the new user account.

Applying a Captive Portal Profile to a Wireless Connection

In order to use a newly created portal profile, you must follow the steps below to apply the captive portal to one of the SSIDs of the device.

Step 1. Navigate to **Wireless > Basic Settings** in the web configuration utility. The *Basic Settings* page appears:

Basic Settings

Radio: Enable

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: 20MHz 20/40MHz

Wireless Channel: Auto

AP Management VLAN: 1

U-APSD (WMM Power Save): Enable

Wireless Table

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	VLAN	Wireless Isolation with SSID	WMM	Max Associated clients	WPS	Captive Portal	
											Portal Profile	Enable
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscosb1	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	<input checked="" type="checkbox"/>	Please select a Profile	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	ciscosb2	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Please select a Profile	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	ciscosb3	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Please select a Profile	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	ciscosb4	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Please select a Profile	<input type="checkbox"/>

Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit WPS

Save Cancel

Step 2. Check the check box next to the SSID you wish to apply the profile to and click **Edit**.

Wireless Table

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	VLAN	Wireless Isolation with SSID	WMM	Max Associated clients	WPS	Captive Portal	
											Portal Profile	Enable
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ciscosb1	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	<input checked="" type="checkbox"/>	Please select a Profile	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	ciscosb2	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Please select a Profile	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	ciscosb3	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Please select a Profile	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	ciscosb4	<input type="checkbox"/>	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Please select a Profile	<input type="checkbox"/>

Edit Edit Security Mode Edit MAC Filtering Time of Day Access Edit WPS

Step 3. Check the **Enable** check box for Captive Portal, and select the profile you would like to use from the *Portal Profile* drop-down list.

st	Security Mode	MAC Filter	VLAN	Wireless Isolation with SSID	WMM	Max Associated clients	WPS	Captive Portal	
								Portal Profile	Enable
	WPA2-Personal	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	16	<input checked="" type="checkbox"/>	Please select a Profile	<input checked="" type="checkbox"/>
	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Please select a Profile	<input type="checkbox"/>
	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	cisco1	<input type="checkbox"/>
	Disabled	Disabled	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	0	<input type="checkbox"/>	Create a new Portal Profile	<input type="checkbox"/>
								Please select a Profile	<input type="checkbox"/>

Note: If guest verification is used on the portal profile, a VLAN other than 1 must be chosen from the VLAN drop-down list. Please refer to [VLAN Membership on RV130 and RV130W](#) if you need help creating a new VLAN.

Step 4. Click **Save** to save your changes.

Note: You must reboot your device afterwards to ensure that captive portal is applied to your network.