

How to Setup Captive Portal - DWC-2000 Wireless Controller

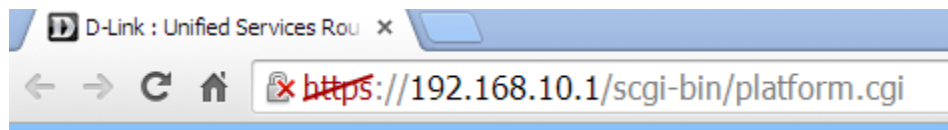
This example will use the following devices and setup:

DWC-2000 – Unified Wireless Controller

DWL-6600AP - Unified Wireless N Simultaneous Dual-Band PoE Access Point



Step 1 – Enter the web GUI interface of the DWC-2000 Wireless Controller using its IP address in a web browser. In our example we have used the IP address of **192.168.10.1**



Accept any certificate warnings you may see, this is perfectly normal and safe

Step 2 – We first now need add a new user group for Captive Portal

Security > User Database > Groups

The screenshot shows the D-Link Unified Controller web interface. At the top, it displays the D-Link logo, 'Unified Controller - DWC 2000', and system information including Serial Number (S3391F3000010), Firmware Version (4.4.0.3_B101_WW), and Language (English [US]). The user is logged in as 'admin (ADMIN)' with a 'Logout' button. A navigation menu includes Status, Wireless, Network, Security, and Maintenance. The breadcrumb trail is 'Security > Authentication > User Database > Groups'. Below this, there are tabs for 'Get User DB', 'Groups', 'Users', 'MAC Authentication', and 'Password Rules'. A message states: 'This page shows the list of added groups to the controller. The user can add, delete and edit the groups also.' The 'Groups List' section shows a table with two entries: 'ADMIN' (Admin Group) and 'GUEST' (Guest Group). Below the table, it says 'Showing 1 to 2 of 2 entries' and includes navigation buttons for 'First', 'Previous', '1', 'Next', and 'Last'. A red box highlights the 'Add New Group' button at the bottom left of the page.

Click **"Add New Group"**

Step 3 – Enter **"Group Configuration"**, please refer to our example below

The screenshot shows the 'Group Configuration' dialog box. It has a title bar with 'Group Configuration' and a close button. The form contains the following fields and options:

- Group Name: CaptivePortal
- Description: Captive Portal Group
- User Type: Radio buttons for Admin, Network (selected), Front Desk, and Guest.
- Captive Portal User: A checkbox that is checked.
- Session Timeout: Input field with '0' and a note '[Default: 0, Range: 0 - 1440] Minutes'.
- Idle Timeout: Input field with '10' and a note '[Default: 10, Range: 1 - 999] Minutes'.

A red box highlights the 'Save' button at the bottom right of the dialog.

Group Name: CaptivePortal

Description: Captive Portal Group

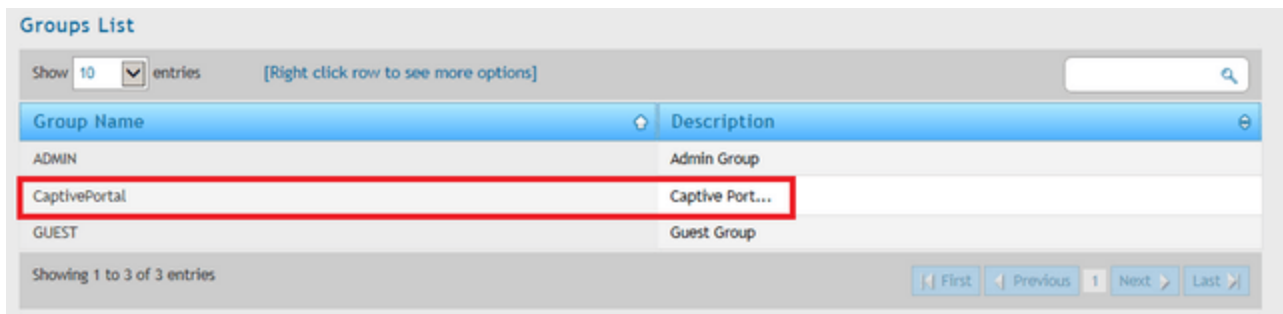
User Type: Network

Captive Portal User: On

Session Timeout: 0

Idle Timeout: 10

Once complete, click **"Save"**



The screenshot shows a web interface titled "Groups List". At the top, there is a search bar and a dropdown menu set to "10" entries. Below this is a table with two columns: "Group Name" and "Description". The table contains three rows: "ADMIN" with description "Admin Group", "CaptivePortal" with description "Captive Port...", and "GUEST" with description "Guest Group". The "CaptivePortal" row is highlighted with a red border. At the bottom of the table, there are navigation buttons: "First", "Previous", "1", "Next", and "Last".

Group Name	Description
ADMIN	Admin Group
CaptivePortal	Captive Port...
GUEST	Guest Group

Step 4 – We now need add new user(s) for Captive Portal

Security > User Database > Users

The screenshot shows the D-Link Unified Controller web interface. The top navigation bar includes 'Status', 'Wireless', 'Network', 'Security', and 'Maintenance'. The breadcrumb trail is 'Security > Authentication > User Database > Users'. Below the breadcrumb, there are tabs for 'Get User DB', 'Groups', 'Users', 'MAC Authentication', and 'Password Rules'. The 'Users' tab is active. A message states: 'This page shows a list of available users in the system. A user can add, delete and edit the users also. This page can also be used for setting policies on users.' Below this is the 'Users List' section, which includes a search bar and a table with the following data:

User Name	Group Name	Login Status
admin	ADMIN	Enabled
guest	GUEST	Disabled

At the bottom left, the 'Add New User' button is highlighted with a red box.

Click **"Add New User"**

Step 5 – Enter **"User Configuration"**, please refer to our example below

The screenshot shows the 'User Configuration' dialog box. The form contains the following fields and values:

- User Name: cp
- First Name: Captive
- Last Name: Portal
- Select Group: CaptivePortal
- Enable Password Change: off
- MultiLogin: on
- Password: [masked]
- Confirm Password: [masked]

A red box highlights the 'Save' button at the bottom right of the dialog.

User Name: cp

First Name: Captive

Last Name: Portal

Select Group: CaptivePortal (This was created in Step 3)

Enable Password Change: Off (Optional)

MultiLogin: On

Password: Enter your password

Confirm Password: Re-enter the above password

Once complete, click **"Save"**



The screenshot shows a 'Users List' interface. At the top, it says 'Show 10 entries' and '[Right click row to see more options]'. There is a search box on the right. The table has three columns: 'User Name', 'Group Name', and 'Login Status'. The rows are: 'admin' (ADMIN, Enabled), 'cp' (CaptivePortal, Enabled), and 'guest' (GUEST, Disabled). The 'cp' row is highlighted with a red border. At the bottom, it says 'Showing 1 to 3 of 3 entries' and has navigation buttons: 'First', 'Previous', '1', 'Next', and 'Last'.

User Name	Group Name	Login Status
admin	ADMIN	Enabled
cp	CaptivePortal	Enabled
guest	GUEST	Disabled

Step 6 – We now need edit the AP Profile and SSID

Wireless > Access Point > AP Profile > AP Profile SSID

AP Profiles | AP Profile Radio | **AP Profile SSID** | AP Profile QoS

This page displays the virtual access point(VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier(SSID). We can configure and enable up to 16 VAPs per radio on each physical access point.

Access Point Profiles SSID List

AP Profile: 1-Default
Radio Mode: 802.11a/n/ac 802.11b/g/n

Show 10 entries [Right click row to see more options]

SSID Name	SSID Status	VLAN	Hide SSID	Security	Redirect	Captive Portal
1-dlink1	Enabled	1-Default	Disabled	VIPA Personal	None	Permanent
2-dlink2	Disabled	1-Default	Disabled	None	None	Free
3-dlink3	Disabled	1-Default	Disabled	None	None	Free
4-dlink4	Disabled	1-Default	Disabled	None	None	Free
5-dlink5	Disabled	1-Default	Disabled	None	None	Free
6-dlink6	Disabled	1-Default	Disabled	None	None	Free
7-dlink7	Disabled	1-Default	Disabled	None	None	Free
8-dlink8	Disabled	1-Default	Disabled	None	None	Free
9-dlink9	Disabled	1-Default	Disabled	None	None	Free
10-dlink10	Disabled	1-Default	Disabled	None	None	Free

Showing 1 to 10 of 16 entries

Right-click over 1-dlink1 and click **"Edit"**

AP Profiles AP Profile Radio **AP Profile SSID** AP Profile QoS

This page displays the virtual access point(VAP) settings associated with the selected AP profile. Each VAP is identified by its network number and Service Set Identifier(SSID). We can configure and enable up to 16 VAPs per radio on each physical access point.

Access Point Profiles SSID List

AP Profile: 1-Default

Radio Mode: 802.11a/n/ac 802.11b/g/n

Show 10 entries [Right click row to see more options]

SSID Name	SSID Status	VLAN	Hide SSID	Security	Redirect	Captive Portal
1-dlink1	Enabled		Disabled	VPA Personal	None	Permanent
2-dlink2	Disabled		Disabled	None	None	Free
3-dlink3	Disabled		Disabled	None	None	Free

Step 7 – Enter a SSID, in our example we have configured as follows:

SSID Configuration

SSID: captiveportal

Captive Portal Type: Permanent User

Enable Redirect: Off

Login Profile Name: default [Create a Profile](#)

Captive Portal Authentication Configuration

Authentication Server: Local User Database

Choose Profile: Login Profile Custom Profile

Hide SSID: Off

Ignore Broadcast: Off

VLAN: 1 [Range: 1 - 4093]

MAC Authentication: Local Radius Disable

Save

SSID Configuration

Redirect: None HTTP

Wireless ARP Suppression Mode: On

L2 Distributed Tunneling Mode: On

Band Steering: On

Radius Server Name: Default-RADIUS-Server

RADIUS Authentication Server Status: Configured

Radius Accounting Server Name: Default-RADIUS-Server

Radius Accounting Server Status: Configured

Save

SSID Configuration

RADIUS Use Network Configuration OFF

Accounting Mode OFF

Security None WPA/WPA2
 WPA Personal WPA Enterprise

WPA Versions

WPA ON OFF

WPA2 ON OFF

WPA Ciphers

TKIP ON OFF

CCMP(AES) ON OFF

WPA Key Type ASCII

Save

SSID Configuration

WPA Key Type ASCII

WPA Key *****

Bcast Key Refresh Rate [Default: 300, Range: 0 - 86400] Seconds

Client QoS OFF

Client QoS Bandwidth Limit Down [0 to 4294967295, 0 - Disable]

Client QoS Bandwidth Limit Up [0 to 4294967295, 0 - Disable]

Client QoS Access Control Down

Client QoS Access Control Up

Save

SSID Configuration

Client QoS OFF

Client QoS Bandwidth Limit Down [0 to 4294967295, 0 - Disable]

Client QoS Bandwidth Limit Up [0 to 4294967295, 0 - Disable]

Client QoS Access Control Down

Client QoS Access Control Up

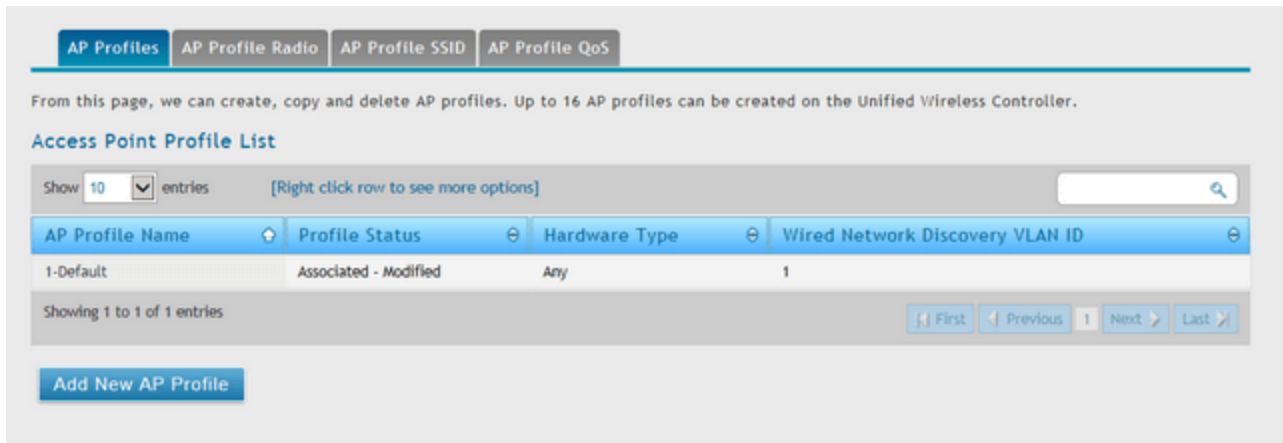
Client QoS Diffserv Policy Down

Client QoS Diffserv Policy Up

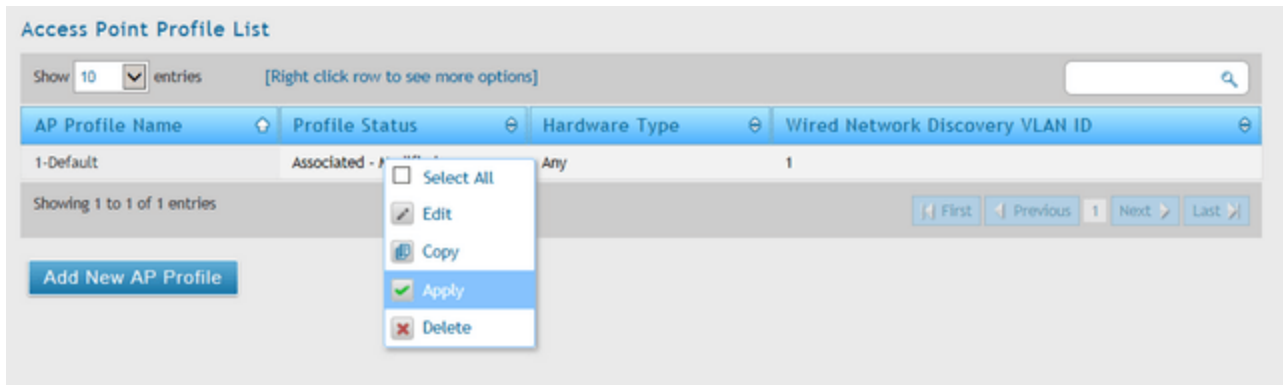
Save

Once complete, click **“Save”**

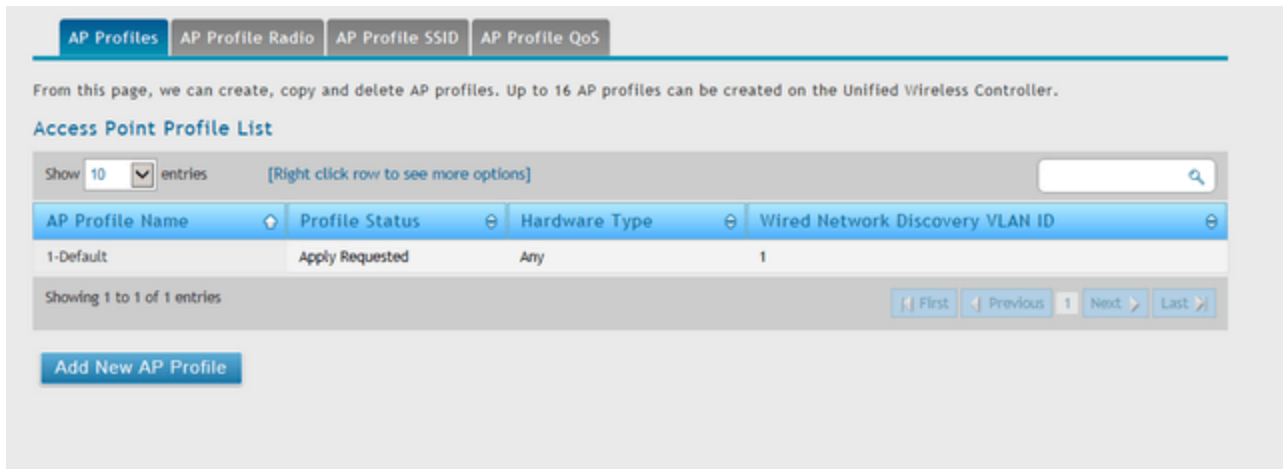
Step 8 – Click on “AP Profiles” and you should notice the default profile has a status of “**Associated-Modified**”



Right-click over the default profile and select “**Apply**”



Step 9 – Once applied the status should show “**Apply Requested**”



Step 10 – When your changes have been successfully applied you should see **“Associated”**

The screenshot shows the 'Access Point Profile List' in a Unified Wireless Controller. At the top, there are tabs for 'AP Profiles', 'AP Profile Radio', 'AP Profile SSID', and 'AP Profile QoS'. Below the tabs, a message states: 'From this page, we can create, copy and delete AP profiles. Up to 16 AP profiles can be created on the Unified Wireless Controller.' The main section is titled 'Access Point Profile List' and contains a table with the following columns: 'AP Profile Name', 'Profile Status', 'Hardware Type', and 'Wired Network Discovery VLAN ID'. The table has one entry: '1-Default', 'Associated', 'Any', and '1'. Below the table, it says 'Showing 1 to 1 of 1 entries' and includes navigation buttons for 'First', 'Previous', 'Next', and 'Last'. There is also a search bar and a link to 'Add New AP Profile'.

AP Profile Name	Profile Status	Hardware Type	Wired Network Discovery VLAN ID
1-Default	Associated	Any	1

Step 11 – Once you have completed the above, you are now able to test the **“Captive Portal”** as follows:

The following was tested with a Nokia Lumia 920 Phone. Once you authenticate against the SSID created in **Step 7** you will be automatically re-directed to the following login screen



• Please Login!!

CAPTIVE PORTAL LOGIN

Username

Password

Login



•Successfully logged in

CAPTIVE PORTAL LOGIN

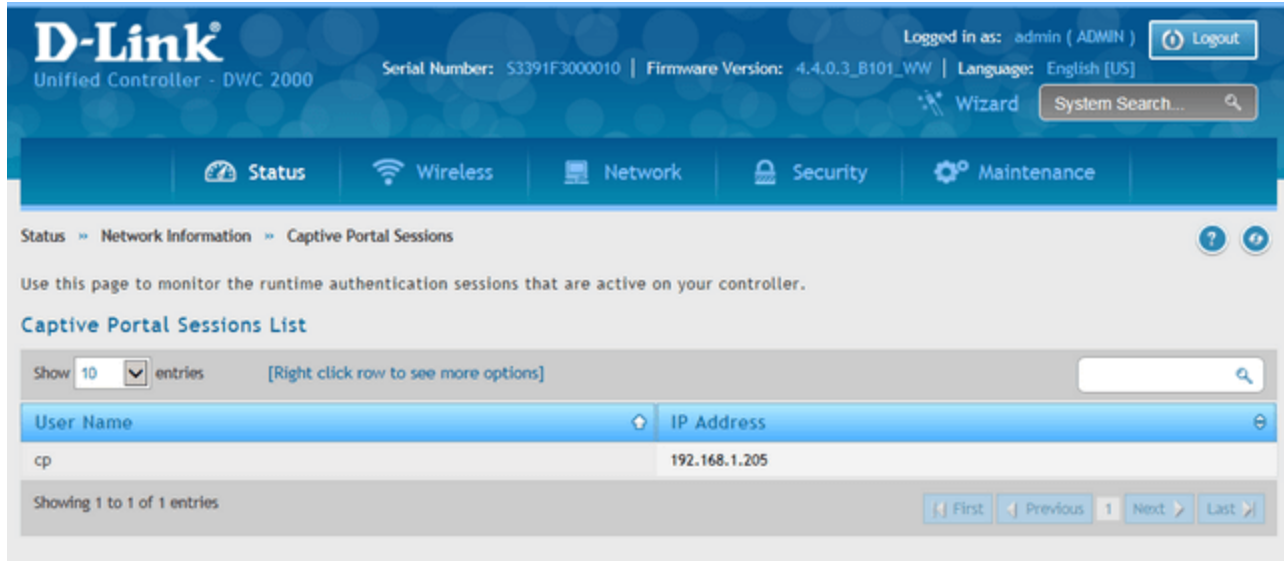
Logout



Additional Notes

When a user is successfully authenticated and connected to the SSID, you are able to monitor and see the users connected by going to the following:

Status > Network Information > Captive Portal Sessions

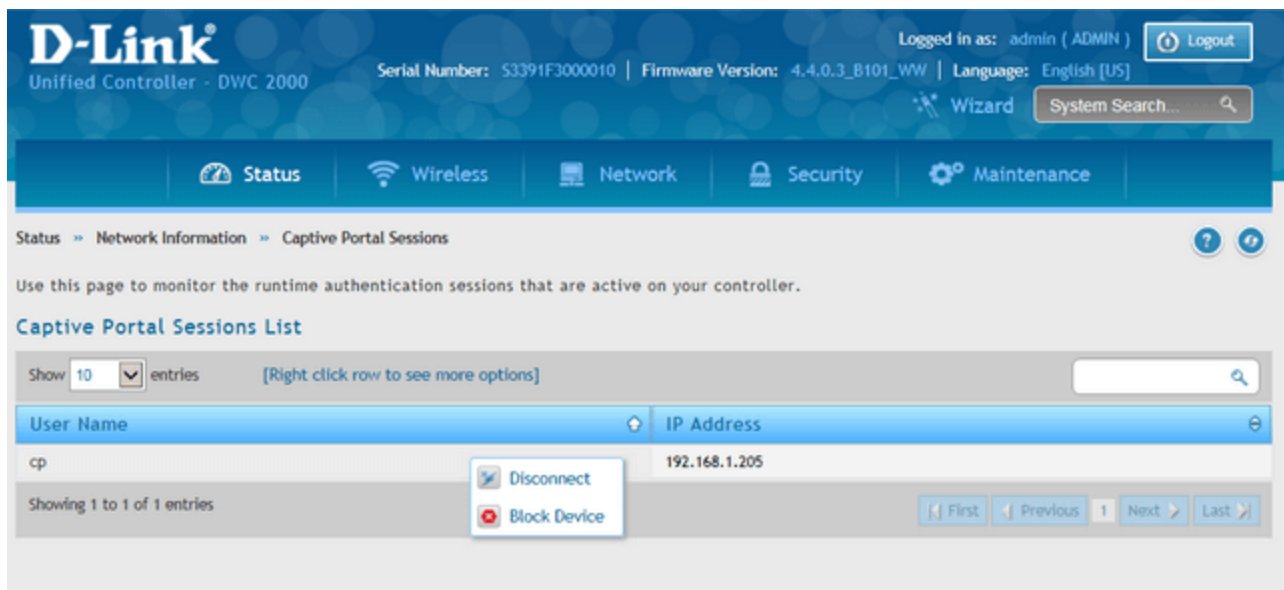


The screenshot shows the D-Link Unified Controller interface. The top navigation bar includes the D-Link logo, 'Unified Controller - DWC 2000', and system information: 'Serial Number: 53391F3000010 | Firmware Version: 4.4.0.3_B101_WW | Language: English [US]'. The user is logged in as 'admin (ADMIN)' with a 'Logout' button. The main navigation menu includes 'Status', 'Wireless', 'Network', 'Security', and 'Maintenance'. The breadcrumb trail is 'Status > Network Information > Captive Portal Sessions'. Below the breadcrumb, there is a description: 'Use this page to monitor the runtime authentication sessions that are active on your controller.' The 'Captive Portal Sessions List' section shows a table with one entry:

User Name	IP Address
cp	192.168.1.205

The table has a search bar and a 'Show 10 entries' dropdown. Below the table, it says 'Showing 1 to 1 of 1 entries' and includes navigation buttons: 'First', 'Previous', '1', 'Next', 'Last'.

You can apply the following actions to the connected users:



This screenshot is identical to the previous one, but with a context menu open over the user 'cp'. The context menu contains two options: 'Disconnect' (with a power icon) and 'Block Device' (with a red stop sign icon).

Right-click over the current user to reveal the following options:

Disconnect – This will disconnect the user from the WLAN

Block Device – This will be remembered and will no-longer be able to connect again (unless you allow)

If you do block a device by accident or you need to unblock, then go to the following menu to un-block device

Security > Firewall > Blocked Clients

Logged in as: admin (ADMIN) Logout

Serial Number: 53391F3000010 | Firmware Version: 4.4.0.3_B101_WW | Language: English [US]

Wizard System Search...

Status Wireless Network Security Maintenance

Security > Firewall > Blocked Clients

This page shows a list of clients MAC addresses blocked by admin.

Block MAC Clients List

Show 10 entries [Right click row to see more options]

MAC Address	Description
54:44:08:24:4c:1c	Blocked

Showing 1 to 1 of 1 entries

First Previous 1 Next Last

Add New Blocked Clients

Right-click over blocked device and select **"Delete"**

Block MAC Clients List

Show 10 entries [Right click row to see more options]

MAC Address	Description
54:44:08:24:4c:1c	Blocked

Showing 1 to 1 of 1 entries

First Previous 1 Next Last

Add New Blocked Clients

- Select All
- Edit
- Delete

Once done, this device will be able to re-join the wireless network and login via the Captive Portal.