D-Link®
Building Networks for People

Version 1.00

Central WiFiManager Configuration Guide

Business Class Networking

Table of Contents

Introduction

This document provides readers with a quick guide that explains the essential operation of the **Central WiFiManager** (CWM). For a more detailed explanation about all the functions in the CWM, refer to the *Central WiFiManager User Manual*.

System Requirements

	Large Scale Deployment	Small Scale Deployment
Maximum APs Managed	1000 APs	100 APs
Recommended CPU	Microsoft® Intel i5 3.2GHz CPU	Microsoft® Intel i3 3.5GHz CPU
Recommended RAM	4G DDR3	2G DDR2
Recommended Storage	2TB	1TB
Ethernet NIC	Gigabit	Gigabit
Display Card	DirectX 11 1GB	DirectX 11 1GB
Windows Platform	Microsoft® Windows 2008 Server Microsoft® Windows 2012 Server	Microsoft® Windows 7 Professional Microsoft® Windows 2008 Server Microsoft® Windows 2012 Server

Access Point Requirement

The following access points are compatible to be managed by the CWM:

- DAP-2310 (H/W: B1, F/W: v2.06rc029 or above)
- DAP-2360 (H/W: B1, F/W: v2.06rc036 or above)
- DAP-2330 (H/W: A1, F/W: v1.06rc020 or above)
- DAP-2660 (H/W: A1, F/W: v1.11rc046 or above)
- DAP-2690 (H/W: B1, F/W: v3.15rc091 or above)
- DAP-2695 (H/W: A1, F/W: v1.15rc050 or above)
- DAP-3662 (H/W: A1, F/W: v1.01rc020 or above)
- DAP-2230 (H/W: A1, F/W: v1.00rc005 or above)
- DAP-3320 (H/W: A1, F/W: v1.00rc011 or above)
- DAP-2553 (H/W: B1, F/W: v3.05rc029 or above)

Latest CWM Modules

The following modules are available and can be installed additionally as add-ons to the CWM:

- CWM_DAP-2310 v2.05-R25
- CWM_DAP-2330 v1.05-R16
- CWM_DAP-2360 v2.05-R19
- CWM_DAP-2660 v1.10-R34
- CWM_DAP-2690 v3.15-R34
- CWM_DAP-2695 v1.15-R37
- CWM_DAP-3662 v1.01-R05
- CWM_DAP-2230 v1.00-R01
- CWM_DAP-3320 v1.00-R02
- CWM_DAP-2553 v3.05-R11

Scenario 1 - Basic Setup

In this scenario we'll configure a very basic Layer 2 edge network configuration with one PC running the Central WiFiManager (CWM) server and two DAP-2660 access points. The objectives in this scenario are as follow:

- To understand the minimum configuration for operation.
- To add access points for CWM management.
- To understand the essential CWM features.

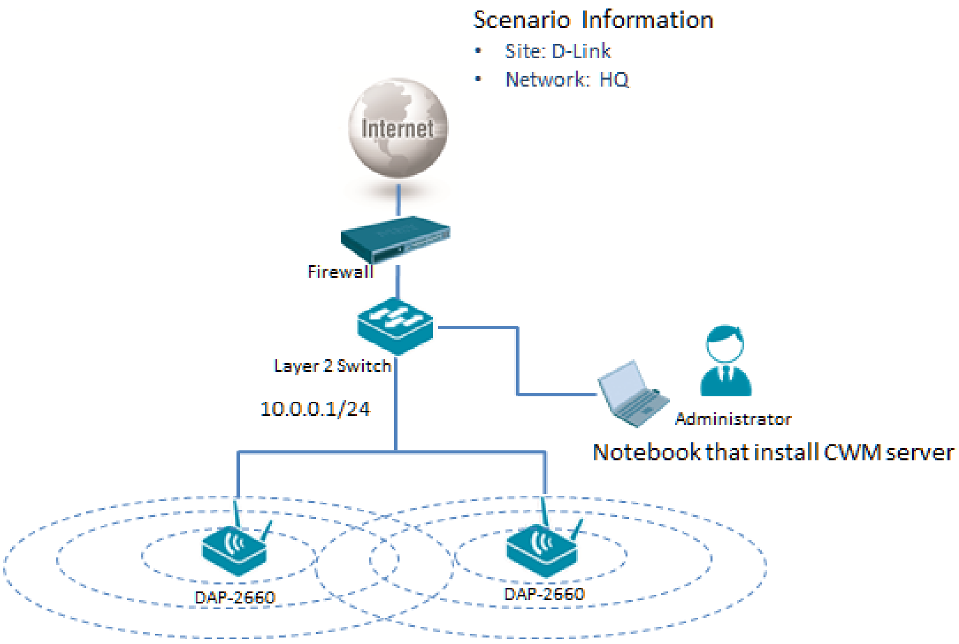


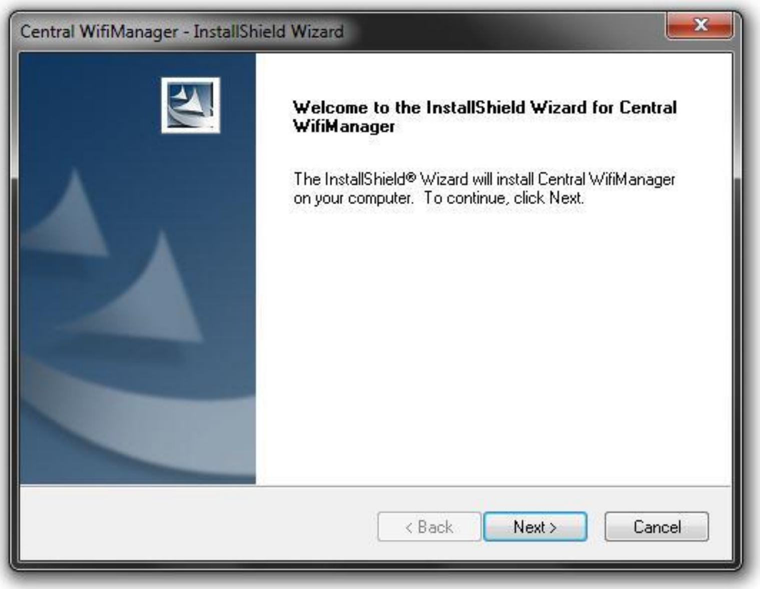
Figure 1-1 Basic Setup Network Layout

The overview of the configuration steps for Central WiFiManager is as follows:

1. Install Central WiFiManager on Computer
2. Install Access Point Module
3. Run the Central WifiManager Server
4. Login to the Central WiFiManager
5. Check and Download AP Module Online
6. Create Site and Network, Configure SSID Settings
7. Add New Access Points in CWM using the AP Installation Utility for CWM

1.1. Install Central WiFiManager on Computer

After running the Central WifiManager installation file (*Central WifiManager v.100.exe*), a welcome window will be displayed.



Central WifiManager - InstallShield Wizard

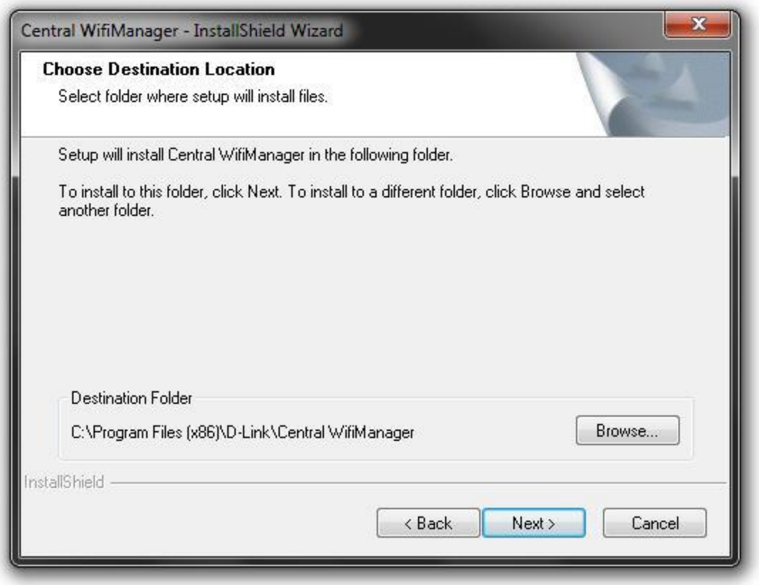
Welcome to the InstallShield Wizard for Central WifiManager

The InstallShield® Wizard will install Central WifiManager on your computer. To continue, click Next.

Figure 1-2 Install Central WifiManager (Welcome)

Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.

In this window, the destination location is displayed, where the software will be installed. If this application needs to be installed at a different location or on a different drive, click the **Browse** button and navigate to the new destination location.



Central WifiManager - InstallShield Wizard

Choose Destination Location

Select folder where setup will install files.

Setup will install Central WifiManager in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

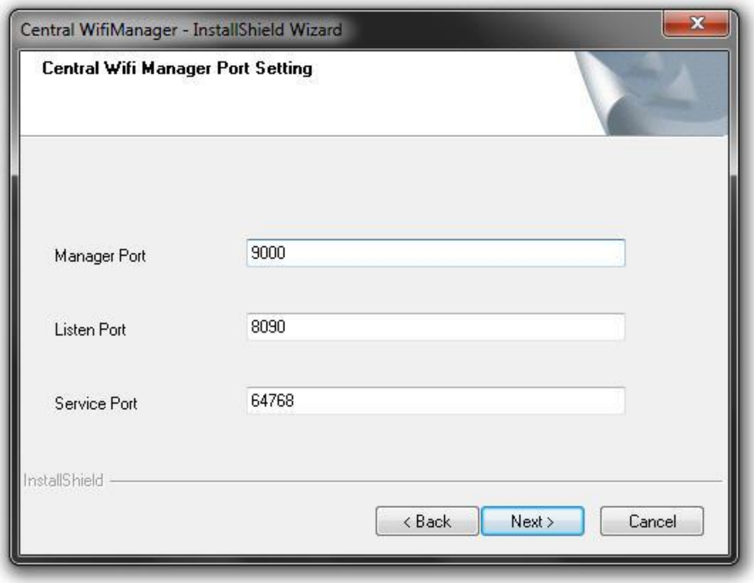
C:\Program Files (x86)\D-Link\Central WifiManager

Figure 1-3 Install Central WifiManager (Destination Location)

Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.

In this window we can change the **Manager Port**, **Listen Port** and **Service Port** numbers. These ports numbers are used for multiple access point connections and it can only be specified here and can’t be modified after the installation. Leave these port numbers on the default settings if these ports have not been used on this computer.

NOTE. Central WiFiManager use HTTPS(TCP 443) for web management.



Central WifiManager - InstallShield Wizard

Central Wifi Manager Port Setting

Manager Port: 9000

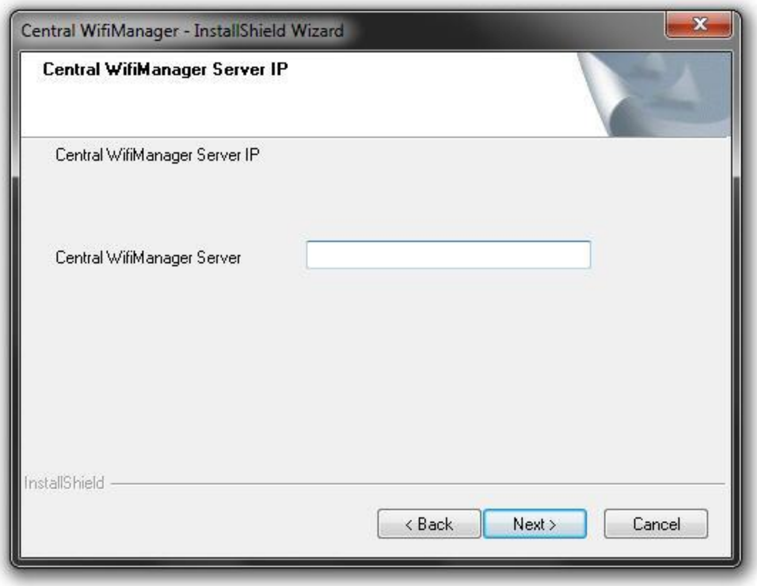
Listen Port: 8090

Service Port: 64768

Figure 1-4 Install Central WifiManager (Port Settings)

Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.

In this window, we need to enter the IP address for the Central WifiManager in the **Central WifiManager Server** space provided. This is normally the IP address of the PC being used for the installation. This IP address can be modified later.



Central WifiManager - InstallShield Wizard

Central WifiManager Server IP

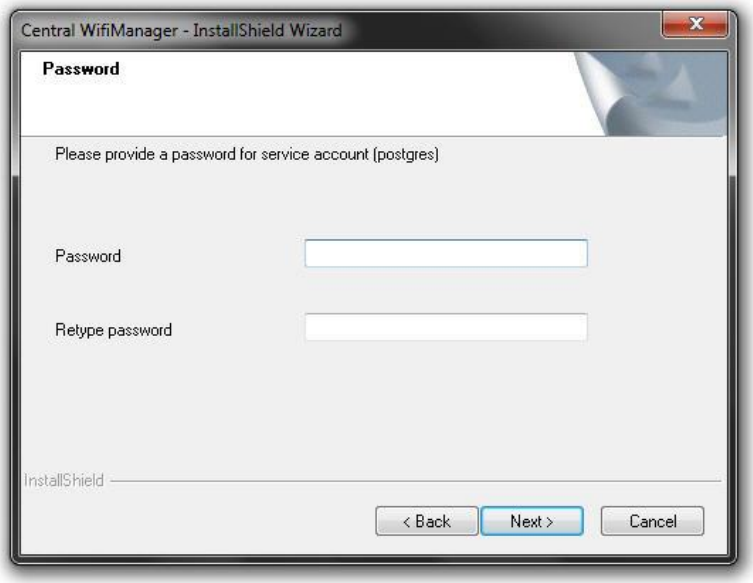
Central WifiManager Server IP

Central WifiManager Server:

Figure 1-5 Install Central WifiManager (Server IP)

Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.

In this window, we must enter the **PostgreSQL** database password that will be associated with this application in the spaces provided. Enter the same password in the **Password** and **Retype password** spaces provided. This password cannot be modified after this installation.



Central WifiManager - InstallShield Wizard

Password

Please provide a password for service account (postgres)

Password

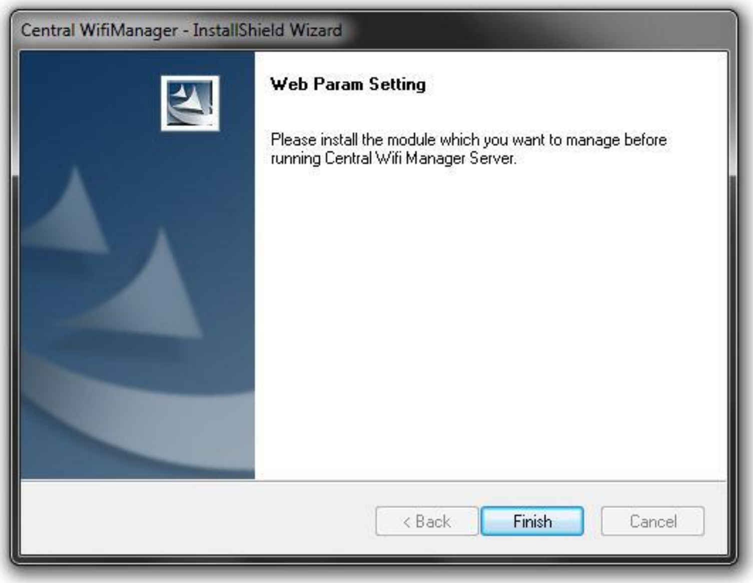
Retype password

Figure 1-6 Install Central WifiManager (Password)

Click the **< Back** button to return to the previous step. Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.

The installation of this application requires **Microsoft Visual C++ 2008 Redistributable** to be installed on this computer. If not found, the option will be given to install the required redistributable. If found this step will be skipped.

The Apache HTTP Server application might be blocked by the computer's firewall. If Windows' default firewall is used, a security alert message will be displayed. Click the **Allow Access** button to allow this application to communicate with the network. In this window, the user is reminded that apart from the Central WifiManager installation, each access point that will be used in this application requires a separate module to be installed. This will be discussed in the next section.



Central WifiManager - InstallShield Wizard

Web Param Setting

Please install the module which you want to manage before running Central Wifi Manager Server.

Figure 1-7 Install Central WifiManager (Finish)

Click the **Finish** button to complete and exit the installation wizard.

After the CWM installation, there will be two applications installed on the PC called the **Central WiFiManager Server** and the **Central WiFiManager**.

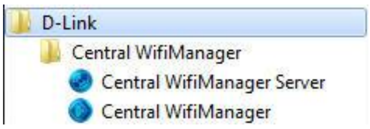
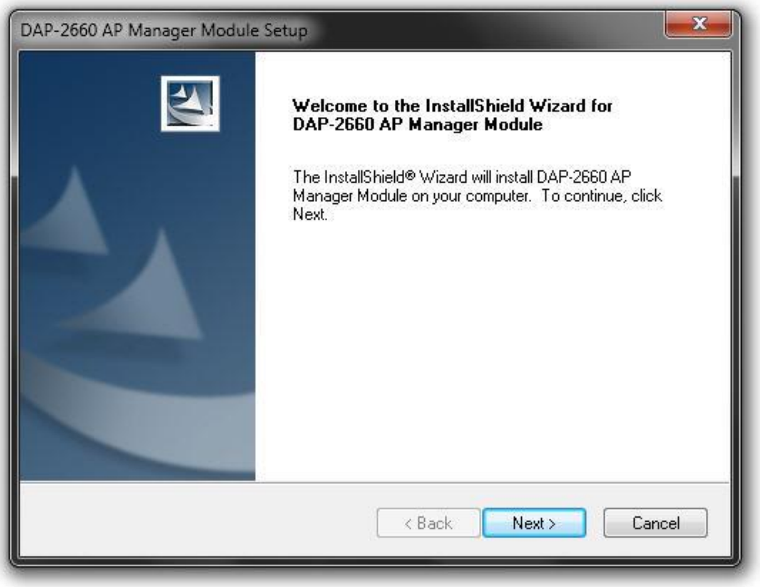


Figure 1-8 Central WifiManager Files

1.2. Install Access Point Module

For each access point that will be used in the D-Link Central WifiManager, we need to install an additional manager module. In this section we'll discuss the installation of the DAP-2660AP access point's manager module that will be used in the D-Link Central WifiManager. If the Central WifiManager Server is already running, it must be stopped and closed before that Access Point manager module can be installed.

After running the access point's manager module, a welcome message will be displayed to inform the user that the manager module will now be installed on the computer.



DAP-2660 AP Manager Module Setup

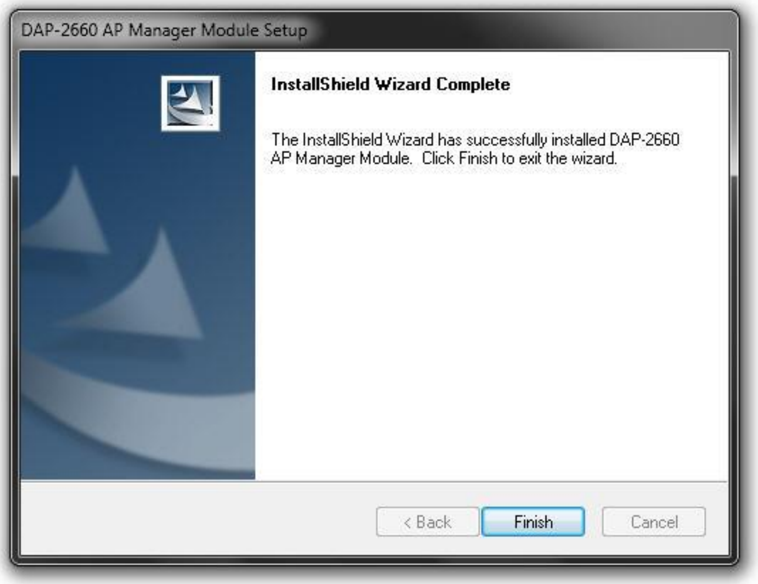
Welcome to the InstallShield Wizard for DAP-2660 AP Manager Module

The InstallShield® Wizard will install DAP-2660 AP Manager Module on your computer. To continue, click Next.

Figure 1-9 Install Access Point Module (Welcome)

Click the **Next >** button to continue to the next step. Click the **Cancel** button to stop and exit the installation.

After the access point's manager module was installed successfully, this window will appear.



DAP-2660 AP Manager Module Setup

InstallShield Wizard Complete

The InstallShield Wizard has successfully installed DAP-2660 AP Manager Module. Click Finish to exit the wizard.

Figure 1-10 Install Access Point Module (Finish)

Click the **Finish** button to complete and exit the installation wizard.

1.3. Run the Central WifiManager Server

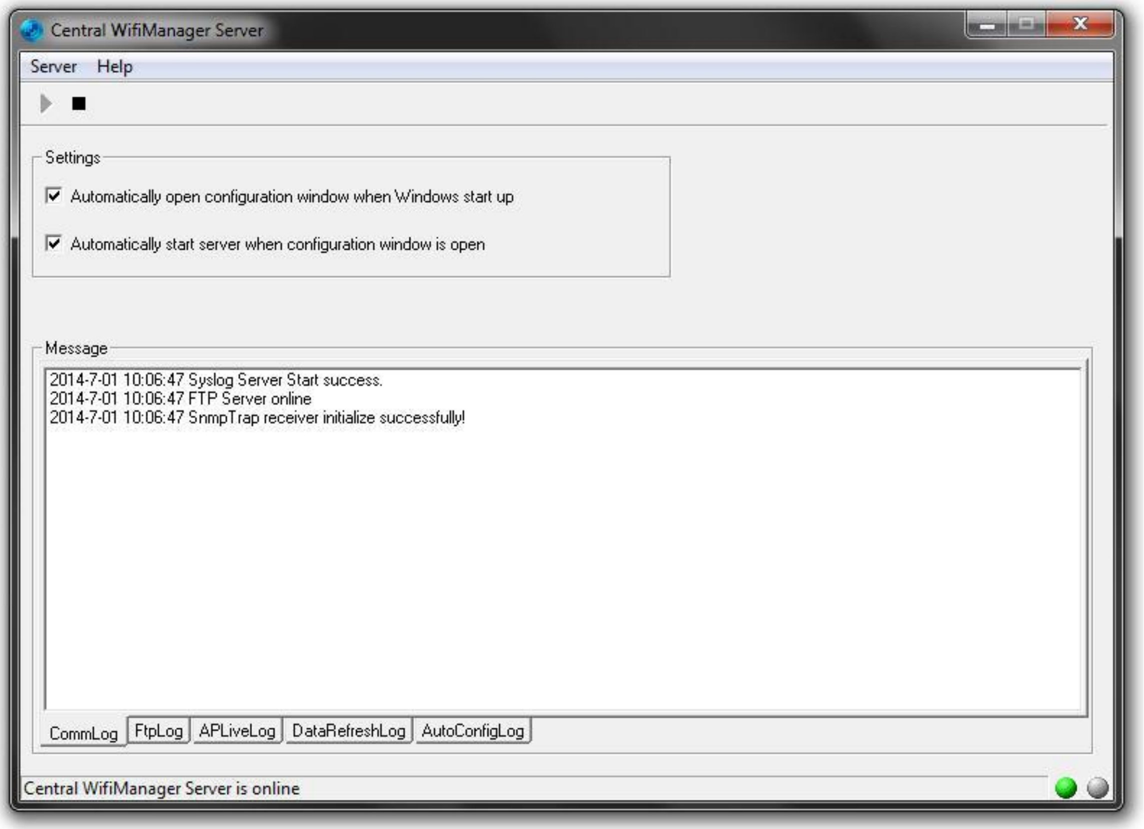
In this section, we'll discuss the Central WifiManager Server application. After the installation was completed the following applications will be available.

Click the Central WifiManager Server option to open the server application.

After running the **Central WifiManager Server** application, the window (on the right) will appear. This is the management console window for the server application.

In the **Menu** bar, there are two options available, **Server** and **Help**. Under the **Server** menu we can **Start**, **Stop** or **Exit** the application. Alternatively, right under the **Server** menu option, there is also start and stop icons. Under the **Help** menu option, there is an **About** option that will, after being clicked, display the name, version and copyright details of this application.

In the **Settings** section, we can select to **Automatically open configuration window when Windows start up** and **Automatically start server when configuration window is open**. Select these options if needed. Click the ▶ icon to start the server.



Central WifiManager Server
Server Help
▶ ■

Settings

☑ Automatically open configuration window when Windows start up

☑ Automatically start server when configuration window is open

Message

```
2014-7-01 10:06:47 Syslog Server Start success.
2014-7-01 10:06:47 FTP Server online
2014-7-01 10:06:47 SnmpTrap receiver initialize successfully!
```

CommLog FtpLog APLiveLog DataRefreshLog AutoConfigLog

Central WifiManager Server is online

Figure 1-11 CWM Management Console

When clicking the close icon (☒), on the far upper right corner, this application will close and exit. The server will not be running in the background. Click the minimize icon (▭) to close this window and allow the server application to run in the background.

When the server is up and running, the left circle icon (🟢), at the far bottom right corner, will display green. When the server is not running the right circle icon (🔴), at the far bottom right corner, will display red.

To view log entries about the System, FTP Connectivity, Live Access Points, Data Transmissions and Automatic Configurations, tabs at the bottom of the **Message** section can be selected.

1.4. Login to the Central WiFiManager

1.4.1. Login to the CWM from a local computer

Click the Central WifiManager option to open the client application(Internet Explorer is the default browser). After the Web browser was open and connection to the server was made successfully, a login window will appear. Enter the login user name, password, CAPTCHA and click **Login** to enter the Central WifiManager configuration.

By default, the user name and password is **admin**.

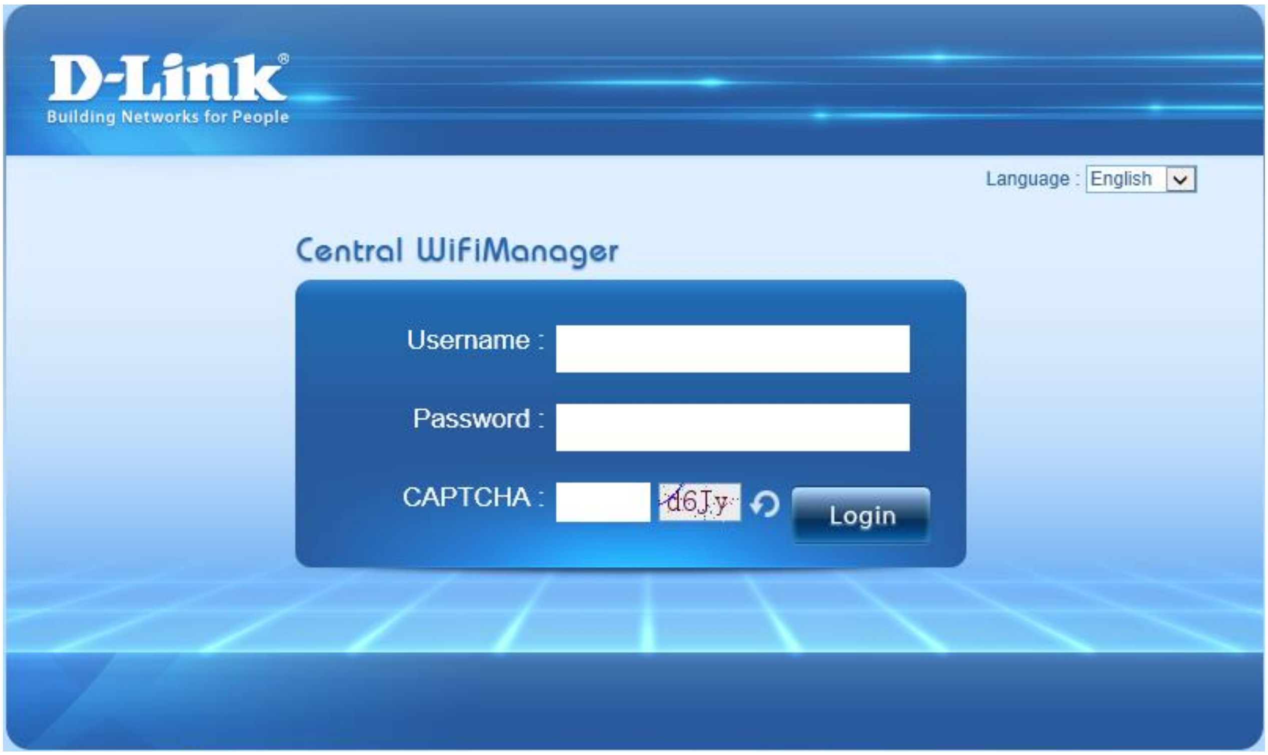


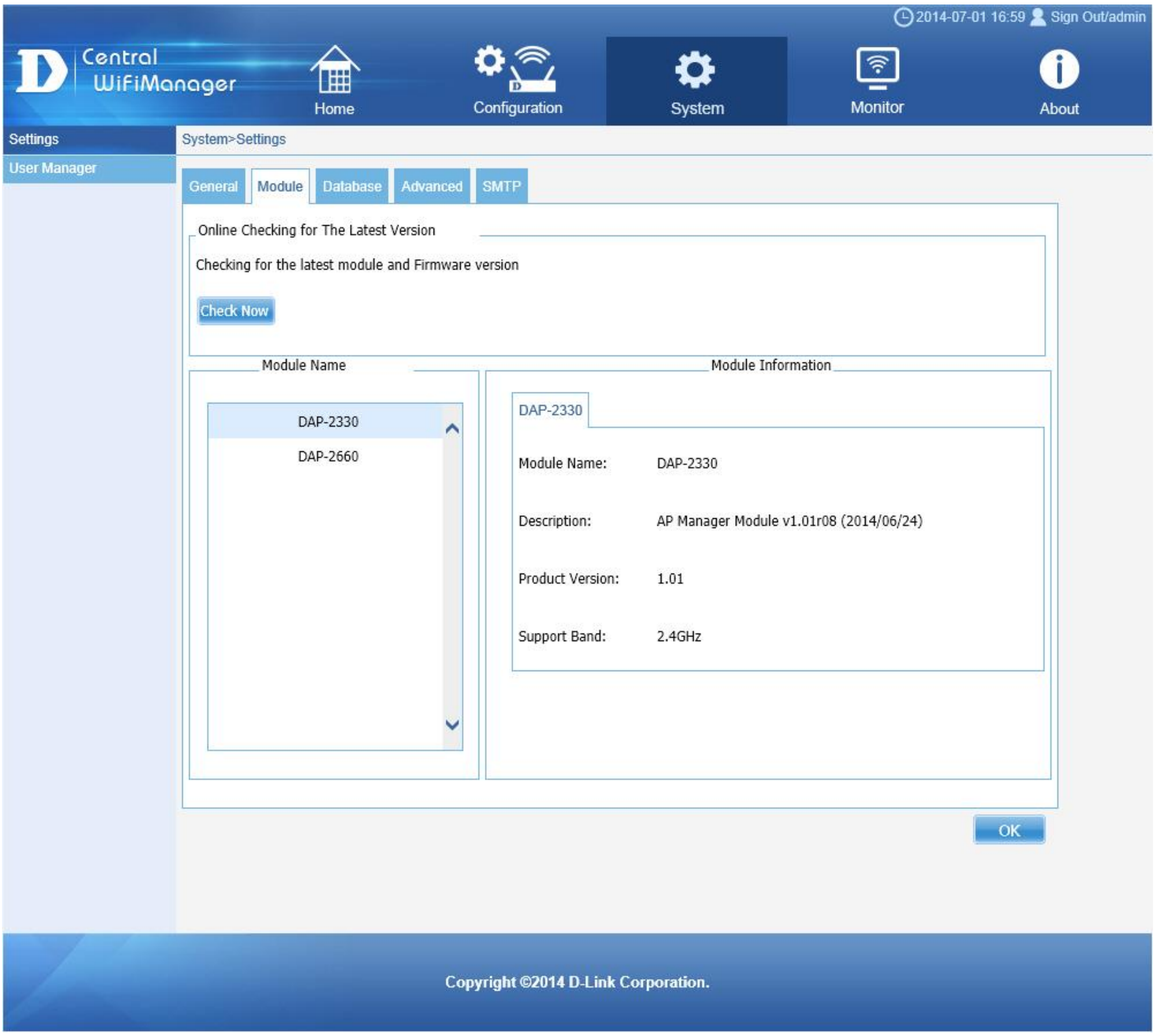
Figure 1-12 CWM Server Login

1.4.2. Remote login Central WiFiManager

Alternatively, from a remote computer, we can connect to the Central WifiManager Server by entering the **IP address** or **Domain Name** of the computer that has the server application installed into the web browser, thus it is not needed to install the software on the remote computer. Open the web browser on the remote computer (Internet Explorer or Google Chrome and Firefox are recommend) and enter for example ***https://192.168.10.1*** or ***https://domain-name.com*** (where ***192.168.10.1*** or ***domain-name.com*** is the IP address or domain name of the computer running the CWM server) in the web browser's address bar and press ***ENTER*** to enter the CWM management interface.

1.5. Check and Download AP Module Online

After logging into the D-Link Central WifiManager Server, we can click on **System**, at the top, then **Settings** on the left, and then select the **Module** tab option, in the middle of the page, to access the following window.



Online Checking for The Latest Version

Checking for the latest module and Firmware version

Module Name

DAP-2330
DAP-2660

Module Information

DAP-2330

Module Name:	DAP-2330
Description:	AP Manager Module v1.01r08 (2014/06/24)
Product Version:	1.01
Support Band:	2.4GHz

Figure 1-13 Update AP Module

In the **Module** tab, a list of access point modules will be displayed in the **Module Name** section. Every different model of access point that can be managed by the Central WifiManager Server requires the administrator to install the executable module file for that specific access point's model name.

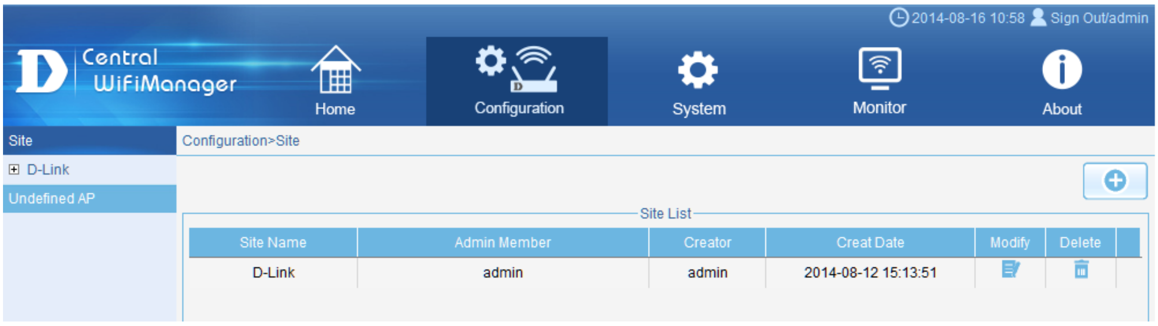
For example, on this page we have two kinds of access point modules installed, the **DAP-2330** and the **DAP-2660**. This means that we can have multiple DAP-2330 and DAP-2660 access points installed on the network, but only required to install two modules, one for each type of access point. The module executable files for all the access points, supported in the application, can be downloaded from the D-Link website.

To keep the installed modules and firmware versions for access points up to date, click on the **Check Now** button.

Click the **OK** button to accept the changes made.

1.6. Create Site and Network, Configure SSID Settings

To create a new **Site** (D-Link), select **Configuration** and then click the ⊕ button. Multiple sites can be created for multi-tenant use.

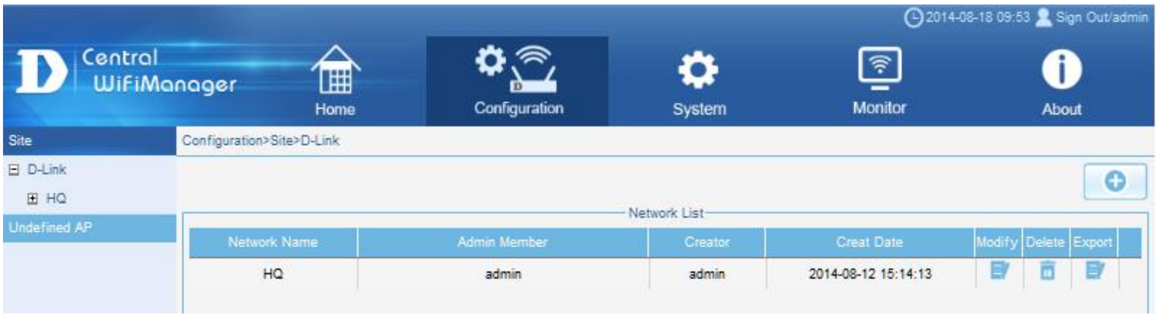


Configuration>Site

Site Name	Admin Member	Creator	Creat Date	Modify	Delete
D-Link	admin	admin	2014-08-12 15:13:51		

Figure 1-14 New Site (D-Link)

To create a new **Network** (HQ), select the newly created **Site** (D-Link) and click the ⊕ button. Multiple networks can be created for each site.

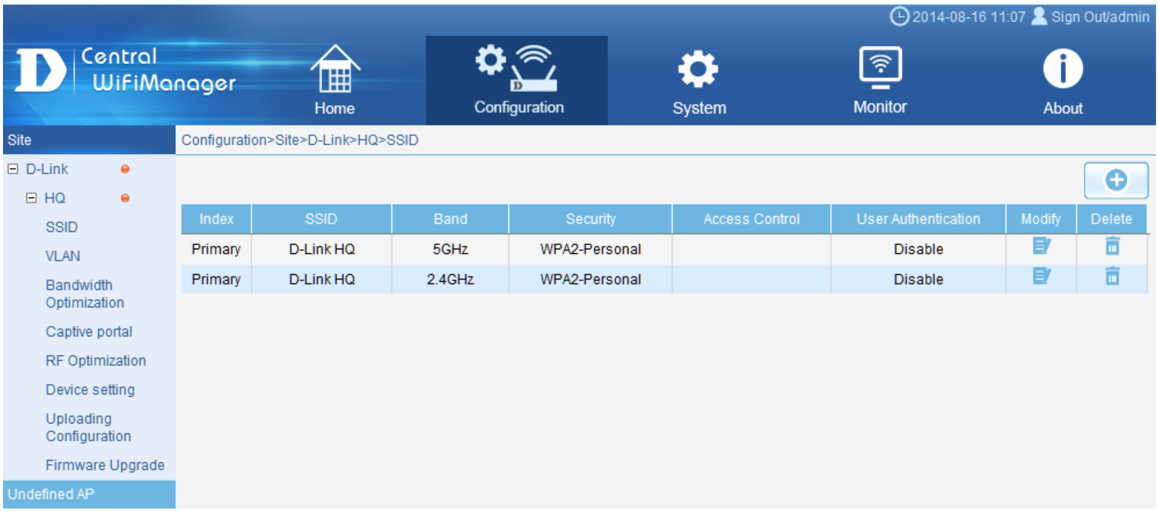


Configuration>Site>D-Link

Network Name	Admin Member	Creator	Creat Date	Modify	Delete	Export
HQ	admin	admin	2014-08-12 15:14:13			

Figure 1-15 New Network (HQ)

After creating the new network (HQ), select it. Additional information will be displayed. For each network additional settings can be configured like **SSID**, **VLAN**, **Bandwidth Optimization**, **RF Optimization**, **Device Settings**, and more.



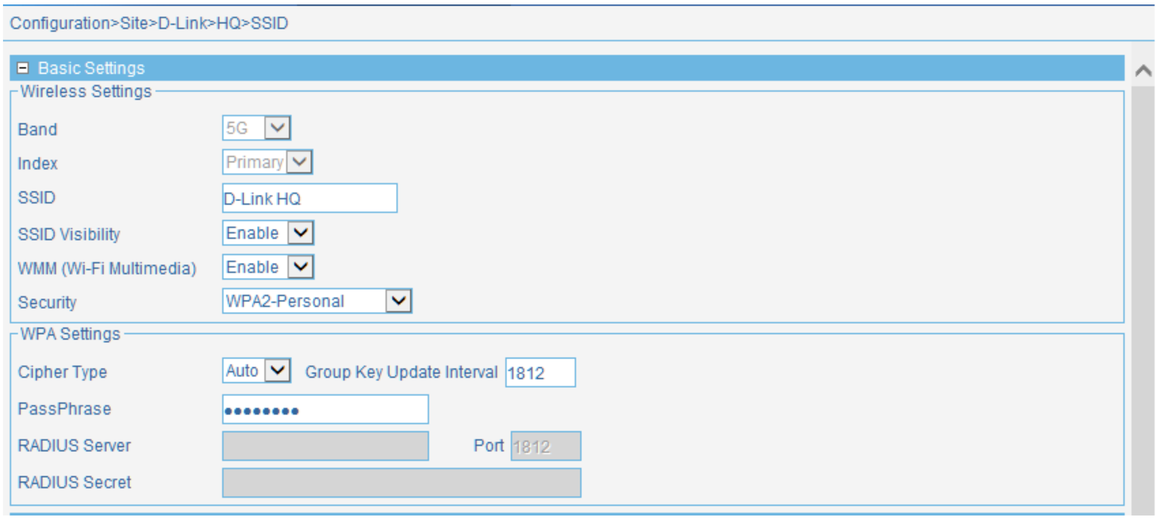
Configuration>Site>D-Link>HQ>SSID

Index	SSID	Band	Security	Access Control	User Authentication	Modify	Delete
Primary	D-Link HQ	5GHz	WPA2-Personal		Disable		
Primary	D-Link HQ	2.4GHz	WPA2-Personal		Disable		

Figure 1-16 Network Configuration Options

To create a new 5GHz **SSID** (D-Link HQ), select the newly created **Network** (HQ) and click the ⊕ button. Select the **Band** (5G), **Index** (Primary), enter the **SSID** (D-Link HQ), and configure the wireless security settings. In this example we used **WPA2-Personal** for wireless security. After selecting WPA-Personal, enter the **PassPhrase** (12345678) in the space provided. Click **Save** to apply the settings.

Note: An orange dot next to a menu option indicates settings that have not been saved (uploaded) to the access point. To finish applying settings, go to “Upload Configuration” from the left menu pane and click “Apply”.



Configuration>Site>D-Link>HQ>SSID

⊟ Basic Settings

Wireless Settings

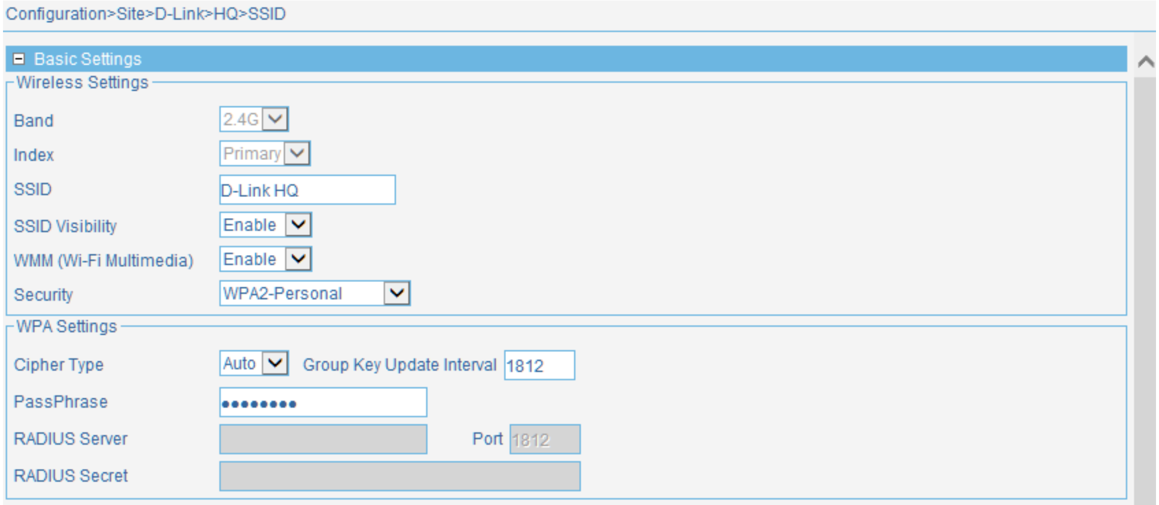
Band: 5G
Index: Primary
SSID: D-Link HQ
SSID Visibility: Enable
WMM (Wi-Fi Multimedia): Enable
Security: WPA2-Personal

WPA Settings

Cipher Type: Auto
Group Key Update Interval: 1812
PassPhrase: ••••••••
RADIUS Server:
Port: 1812
RADIUS Secret:

Figure 1-17 New SSID (5G)

To create a new 2.4GHz **SSID** (D-Link HQ), select the newly created **Network** (HQ) and click the ⊕ button. Select the **Band** (2.4G), **Index** (Primary), enter the **SSID** (D-Link HQ), and configure the wireless security settings. In this example we used **WPA2-Personal** for wireless security. After selecting WPA-Personal, enter the **PassPhrase** (12345678) in the space provided. Click **Save** to apply the settings.



Configuration>Site>D-Link>HQ>SSID

⊟ Basic Settings

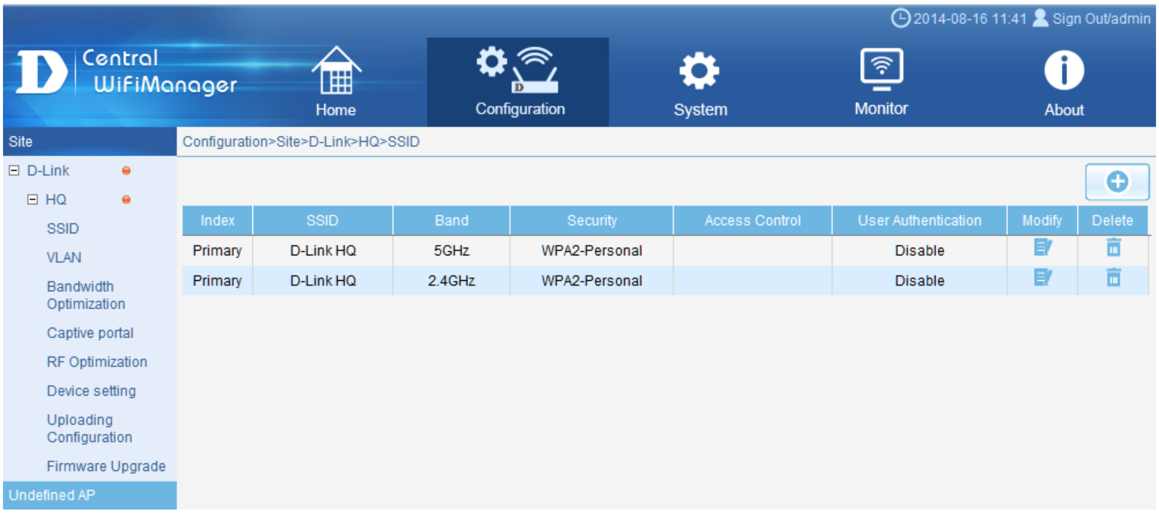
Wireless Settings

Band: 2.4G
Index: Primary
SSID: D-Link HQ
SSID Visibility: Enable
WMM (Wi-Fi Multimedia): Enable
Security: WPA2-Personal

WPA Settings

Cipher Type: Auto
Group Key Update Interval: 1812
PassPhrase: ••••••••
RADIUS Server:
Port: 1812
RADIUS Secret:

Figure 1-18 New SSID (2.4G)



Configuration>Site>D-Link>HQ>SSID

Index	SSID	Band	Security	Access Control	User Authentication	Modify	Delete
Primary	D-Link HQ	5GHz	WPA2-Personal		Disable		
Primary	D-Link HQ	2.4GHz	WPA2-Personal		Disable		

Figure 1-19 Network's SSID List

Because this configuration wasn't uploaded to the access points in this network, red circle icons (●) will be displayed right next to the **Network** (D-Link) and **Site** (HQ) names.

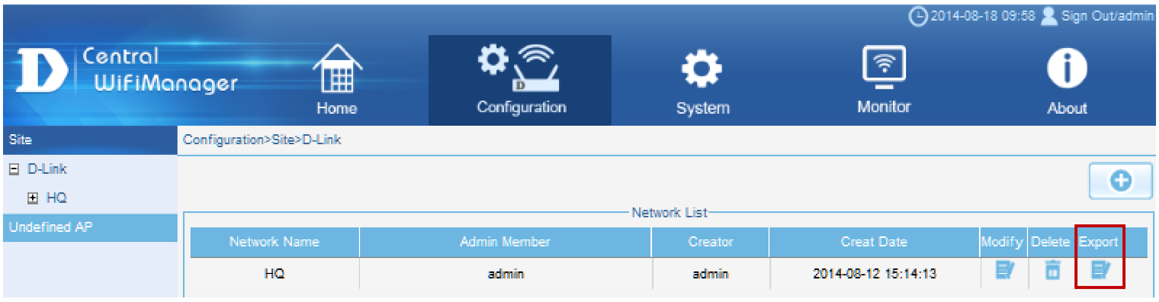
To add new Access Points into the CWM, we need to run Access Point Installation Utility for CWM first. This is required to provide initial synchronization (IP address of the CWM server and authentication information) of APs with the CWM. Once the APs are synchronized with CWM, we can use the CWM: 'Uploading Configuration' option, to push new configuration or any amended configuration remotely to the APs.

Next two sections will explain these options in detail.

1.7. Add New Access Points in CWM using the AP Installation Utility for CWM

1.7.1. Export Network Profile from CWM to your Computer

To add new access points to the CWM, we have to export the network profile from CWM first. The exported file includes the authentication key and the IP address of the controller. Select **Configuration** and then click the **Export** (📝) icon to export the network profile to your computer.



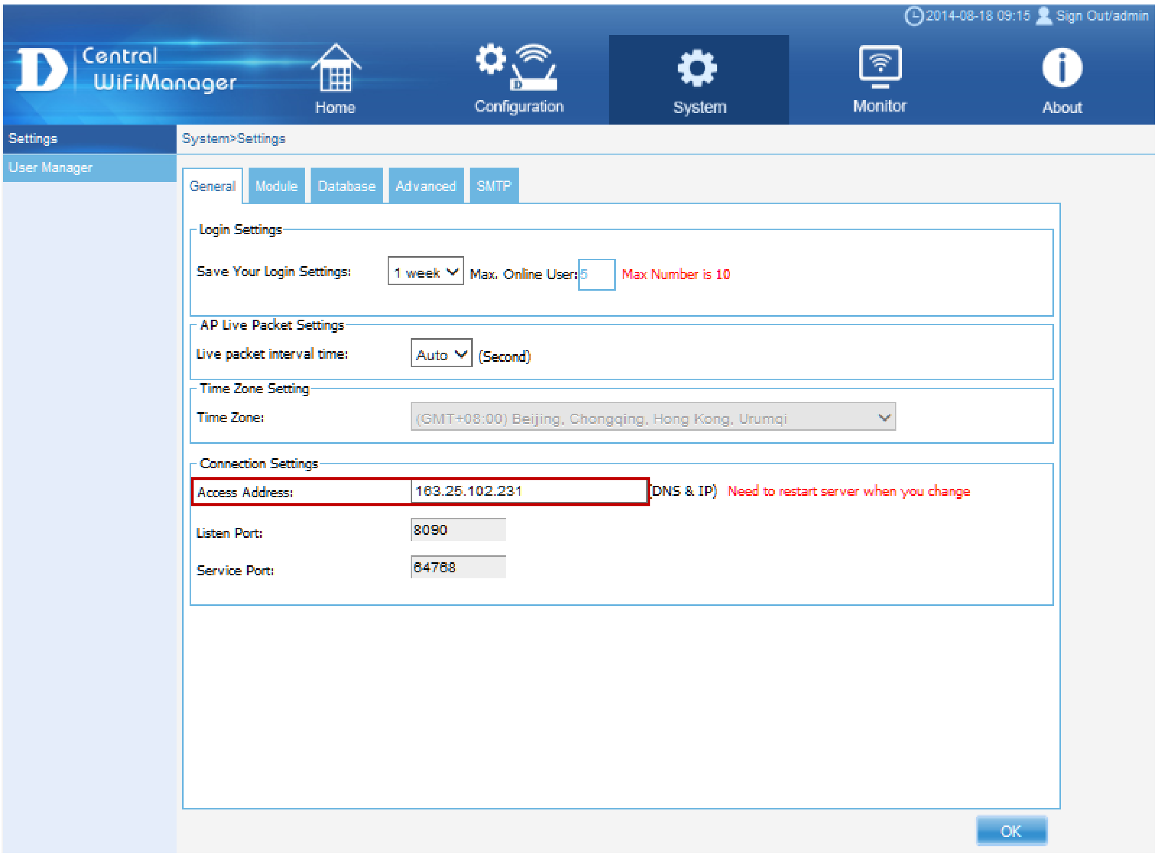
Configuration>Site>D-Link

Network List

Network Name	Admin Member	Creator	Creat Date	Modify	Delete	Export
HQ	admin	admin	2014-08-12 15:14:13	📝	🗑	📝

Figure 1-20 Export Network Profile

When access points are located on a public site and access to the CWM is over the Internet, ensure that the **Access Address** for the CWM is a **public** IP address or domain name and not a private IP address. To verify the Access Address navigate to **System > General > Connection Settings** and double check the **Access Address** field.



System>Settings

Login Settings

Save Your Login Settings: 1 week Max. Online User: 5 Max Number is 10

AP Live Packet Settings

Live packet interval time: Auto (Second)

Time Zone Setting

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

Connection Settings

Access Address: 163.25.102.231 (DNS & IP) Need to restart server when you change

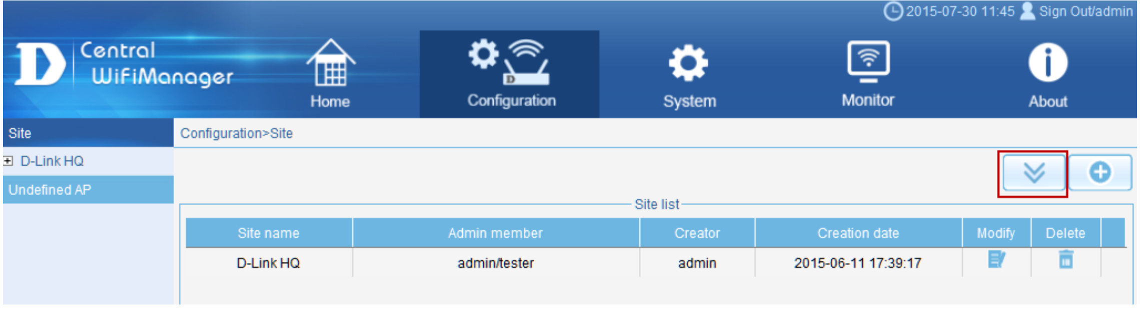
Listen Port: 8090

Service Port: 64768

Figure 1-21 Modify Access Address

1.7.2. Discover and Import the Profile to APs using the Installation Tool

The **Access Point Installation Utility for CWM** is an additional utility that compliments the D-Link Central WifiManager, it can be download from **Configuration>Site** page**.**



2015-07-30 11:45 Sign Out/admin

Site
⊞ D-Link HQ
Undefined AP

Configuration>Site

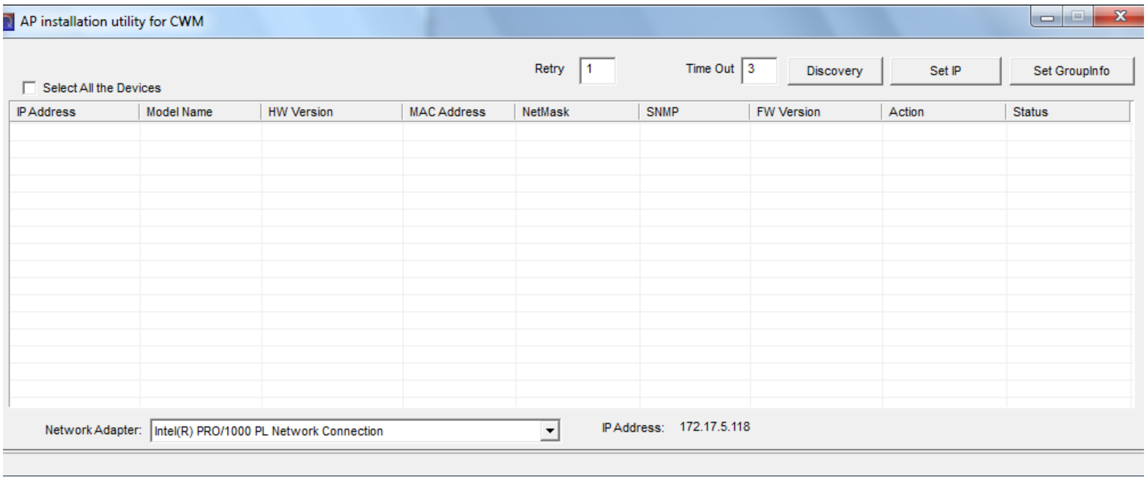
Site list

Site name	Admin member	Creator	Creation date	Modify	Delete
D-Link HQ	admin/tester	admin	2015-06-11 17:39:17		

Figure 1-22 Download the utility for CWM

This utility can be used to scan for new D-Link access points in the local (Layer 2) network, regardless of what IP range they are configured in, and then pre-configure them to be used in the Central WifiManager. This utility will not find access points across a Layer 3 environment. Ensure that the exported network profile file is ready on the computer running this utility.

After opening the Access Point Installation Tool, the following window will be available. Click the **Discovery** button, to scan for D-Link access points that are connected to the network with an Ethernet cable.



AP installation utility for CWM

Retry: 1
Time Out: 3

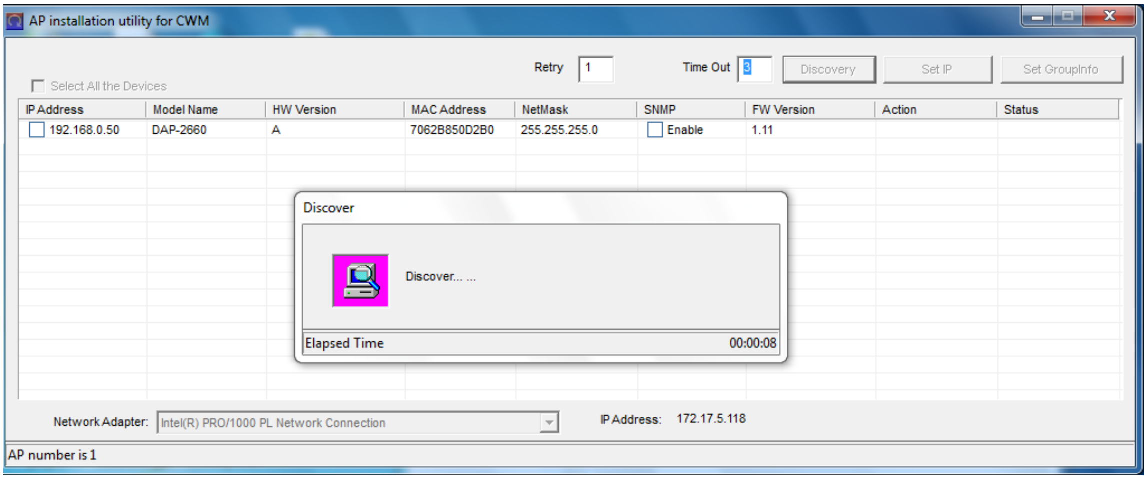
□ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status

Network Adapter: Intel(R) PRO/1000 PL Network Connection
IP Address: 172.17.5.118

Figure 1-23 AP Installation Tool (Open)

After clicking the **Discovery** button, this utility will scan the LAN (Layer 2) network for D-Link access points that are connected to the network with an Ethernet cable.



AP installation utility for CWM

Retry: 1
Time Out: 3

□ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
□ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	□ Enable	1.11		

Discover

Discover... ...

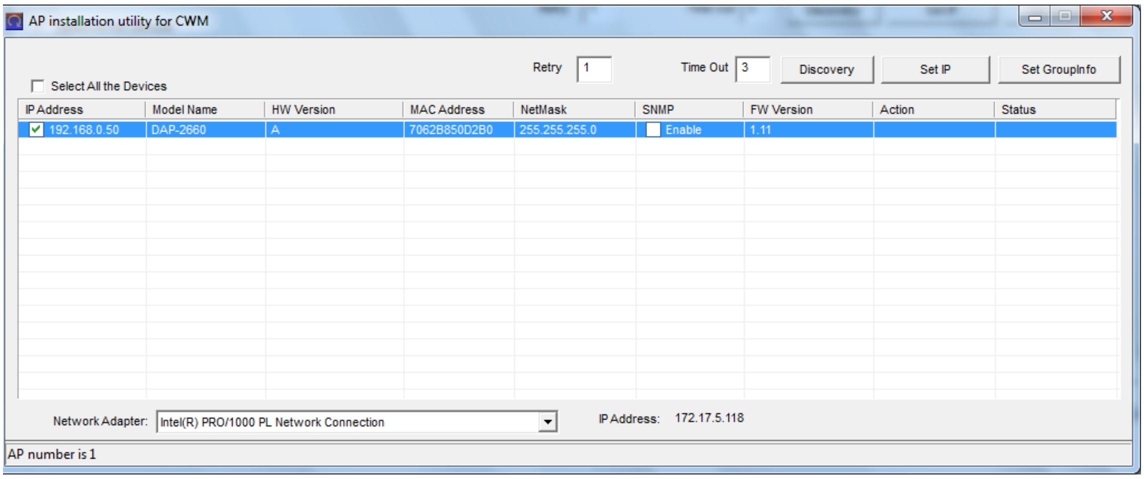
Elapsed Time 00:00:08

Network Adapter: Intel(R) PRO/1000 PL Network Connection
IP Address: 172.17.5.118

AP number is 1

Figure 1-24 AP Installation Utility for CWM (Discover)

After this utility found access point, they will be displayed and can be configured.If the FW version is not latest version(See page 3), please go to acess point’s web page and upload latest firmware first.



AP installation utility for CWM

Retry: 1 Time Out: 3 Discovery Set IP Set GroupInfo

□ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
☑ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	□ Enable	1.11		

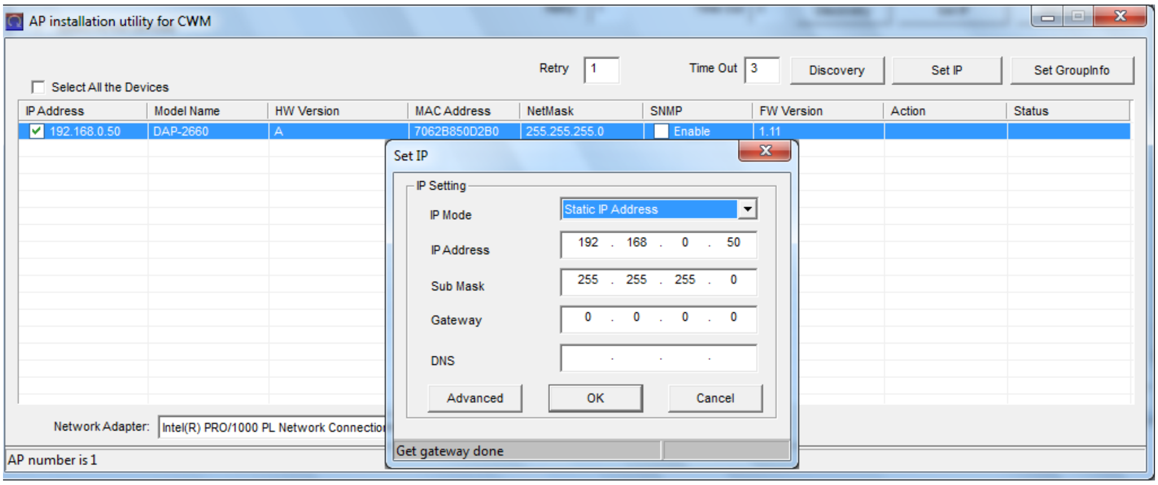
Network Adapter: Intel(R) PRO/1000 PL Network Connection

IP Address: 172.17.5.118

AP number is 1

Figure 1-25 AP Installation Utility for CWM (Found)

To modify the IP address of the newly discovered access point, select it and click the **Set IP** button. Enter the new IP address, subnet mask, gateway address and primary DNS address in the spaces provided. Click **OK** to accept the changes made.



AP installation utility for CWM

Retry: 1 Time Out: 3 Discovery Set IP Set GroupInfo

□ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
☑ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	□ Enable	1.11		

Set IP

IP Setting

IP Mode: Static IP Address

IP Address: 192 . 168 . 0 . 50

Sub Mask: 255 . 255 . 255 . 0

Gateway: 0 . 0 . 0 . 0

DNS: . . .

Advanced OK Cancel

Get gateway done

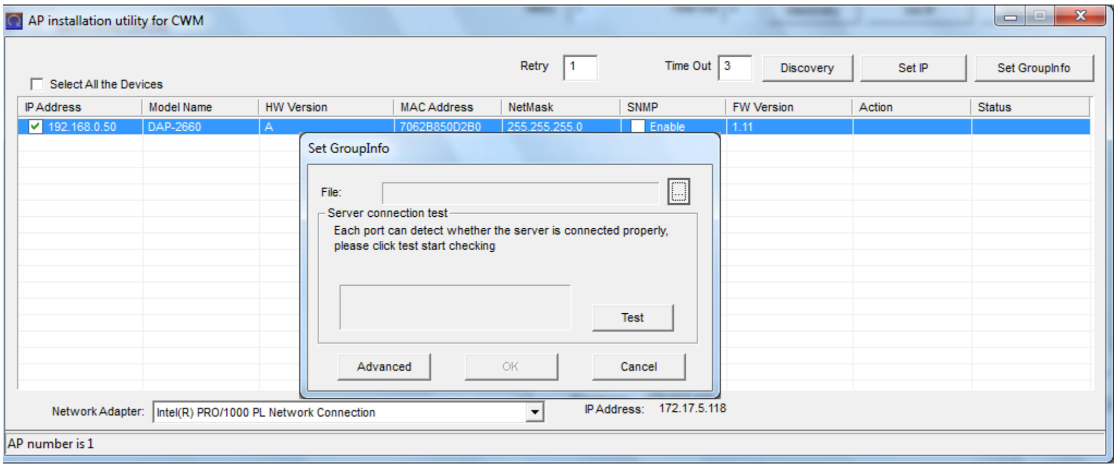
Network Adapter: Intel(R) PRO/1000 PL Network Connectio

AP number is 1

Figure 1-26 AP Installation Utility for CWM (Set IP)

After clicking the **OK** button to set the IP address settings, the access point will be configured and some time will be given for the access point to restart after the new IP address settings was applied. The **Status** parameter will display the progress of the IP address configuration and access point reboot.

This utility also allows us to upload the network data file directly to the access point to configure the group information that this access point will use to identify in which network it belongs. Click the **Set GroupInfo** button to upload the network data file. After click the **Set GroupInfo** button, we can click on the "**...**" button to navigate to the saved network data file on the computer and then upload it.



AP installation utility for CWM

Retry: 1 Time Out: 3 Discovery Set IP Set GroupInfo

□ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
☑ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	□ Enable	1.11		

Set GroupInfo

File:

Server connection test

Each port can detect whether the server is connected properly, please click test start checking

Test

Advanced OK Cancel

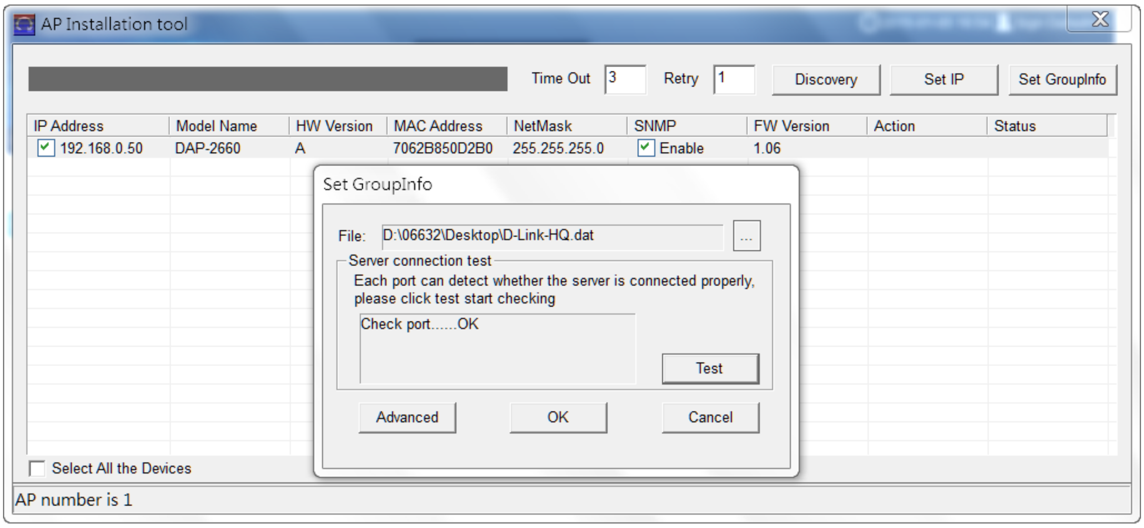
Network Adapter: Intel(R) PRO/1000 PL Network Connection

IP Address: 172.17.5.118

AP number is 1

Figure 1-27 AP Installation Utility for CWM (Set Groupinfo)

Click the **Test** button to test if the data file is in fact a valid network data file. After clicking the **Test** button to successfully test if the network data file is valid, the following message will be displayed. Click the **OK** button to initiate the upload.



AP Installation tool

Time Out 3 Retry 1 Discovery Set IP Set GroupInfo

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
☑ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	☑ Enable	1.06		

Set GroupInfo

File: D:\06632\Desktop\D-Link-HQ.dat ...

Server connection test

Each port can detect whether the server is connected properly, please click test start checking

Check port......OK

Test

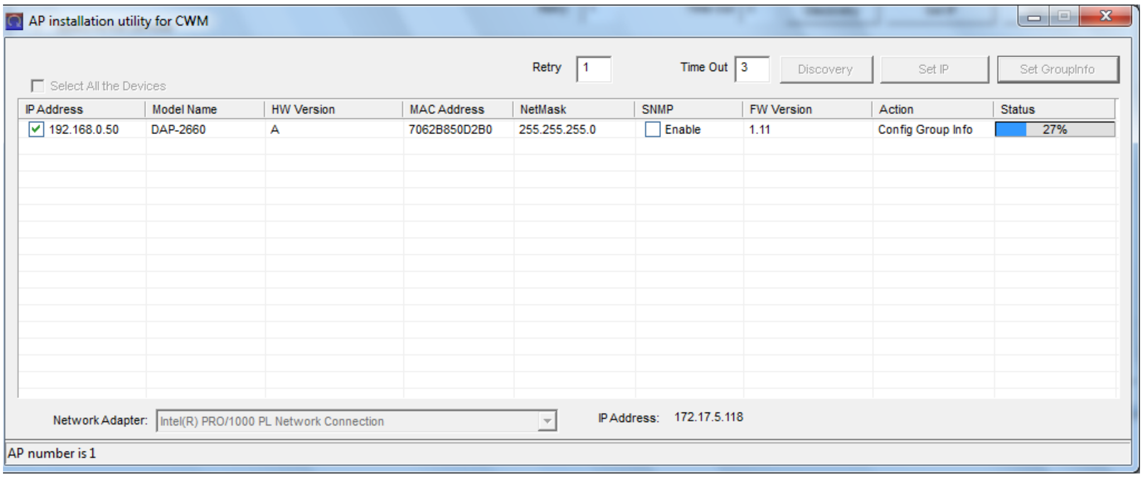
Advanced OK Cancel

□ Select All the Devices

AP number is 1

Figure 1-28 AP Installation Utility for CWM (Test, OK)

After clicking the **OK** button, the network data file will be uploaded, the access point will be configured based on the settings within the data file, and will then reboot. The **Status** parameter will display the progress of the configuration.



AP installation utility for CWM

□ Select All the Devices

Retry 1 Time Out 3 Discovery Set IP Set GroupInfo

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
☑ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	□ Enable	1.11	Config Group Info	27%

Network Adapter: Intel(R) PRO/1000 PL Network Connection

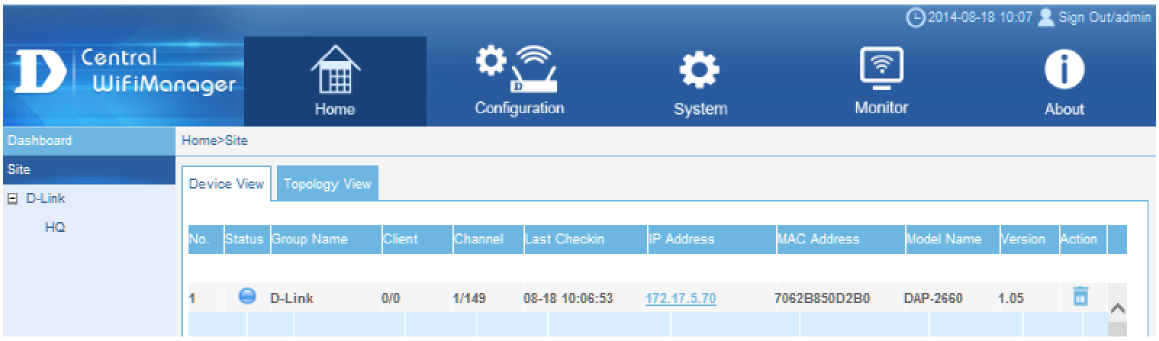
IP Address: 172.17.5.118

AP number is 1

Figure 1-29 AP Installation Utility for CWM (Uploading, Reboot)

1.7.3. Verify Access Points Managed by the CWM

To verify which access points are connected to which sites, navigate to **Home > Network** (Site) **> Site** (D-Link). Online access point will display a blue icon (🔵) in the **Status** field and offline access point will display a grey icon (⚪) in the **Status** field.



Home>Site

No.	Status	Group Name	Client	Channel	Last Checkin	IP Address	MAC Address	Model Name	Version	Action
1	🔵	D-Link	0/0	1/149	08-18 10:06:53	172.17.5.70	7062B850D2B0	DAP-2660	1.05	

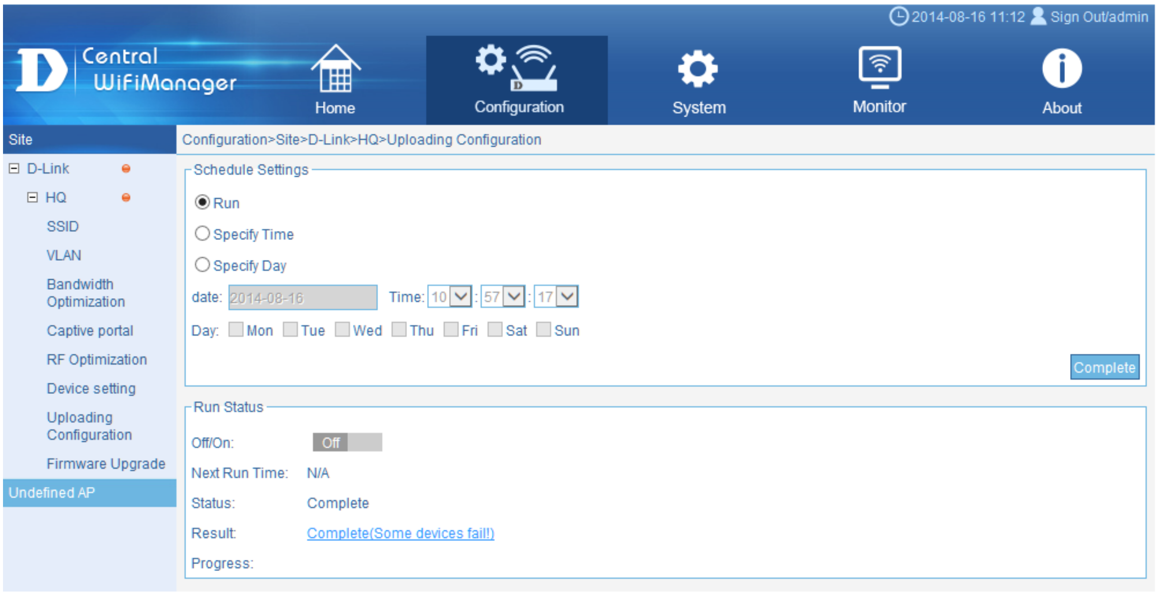
Figure 1-30 Verify Access Points

Additional information displayed for each access point on this page is the **Group Name**, **Client**, **Channel**, **Last Check-in**, **Channel**, **IP Address**, **MAC Address**, **Model Name** and firmware **Version**.

1.8. Uploading New Configuration or Amending existing Configuration

To upload the new configuration to existing access points in the network select the **Uploading Configuration** option, on the left, and then select the **Run** option, and then click the **Complete** button to apply the new settings to the existing access points immediately.

In the **Uploading Configuration** page we can decide whether we need to apply the new configuration to existing access point in the network immediately or by schedule.



Configuration>Site>D-Link>HQ>Uploading Configuration

Schedule Settings

● Run

○ Specify Time

○ Specify Day

date: 2014-08-16 Time: 10 : 57 : 17

Day: □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Run Status

Off/On: Off

Next Run Time: N/A

Status: Complete

Result: Complete(Some devices fail!)

Progress:

Figure 1-31 Uploading Configuration

Scenario 2 - Captive Portal and User Authentication

The **Captive Portal** can provide wireless access to guest users. This feature is frequently used in enterprise, campus and hospital network environments. The objectives in this scenario are as follow:

- Understand how to use captive portal
- Understand how to configure local data base and passcode authentication.

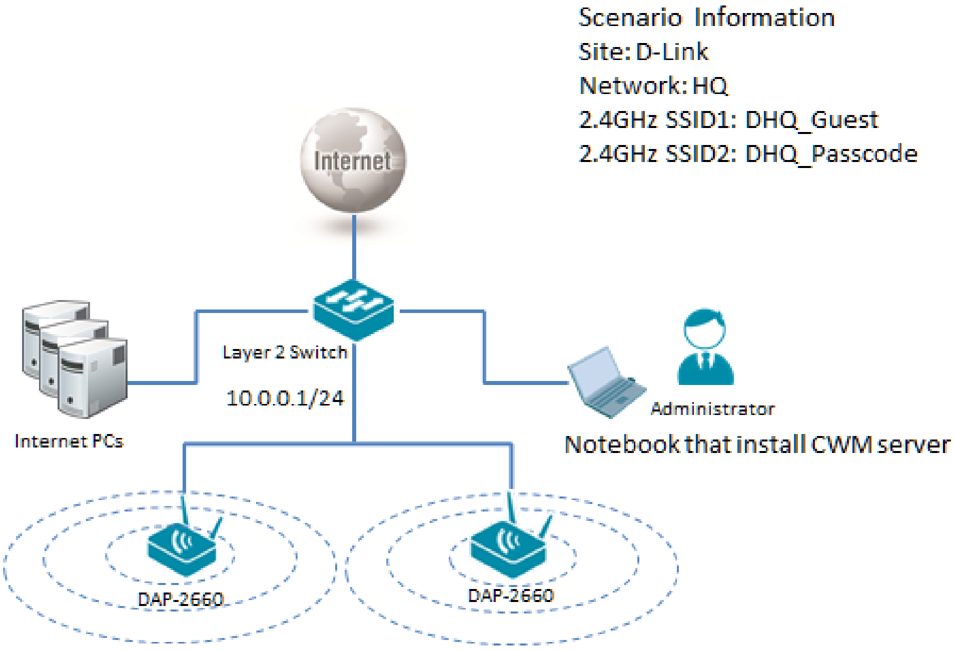


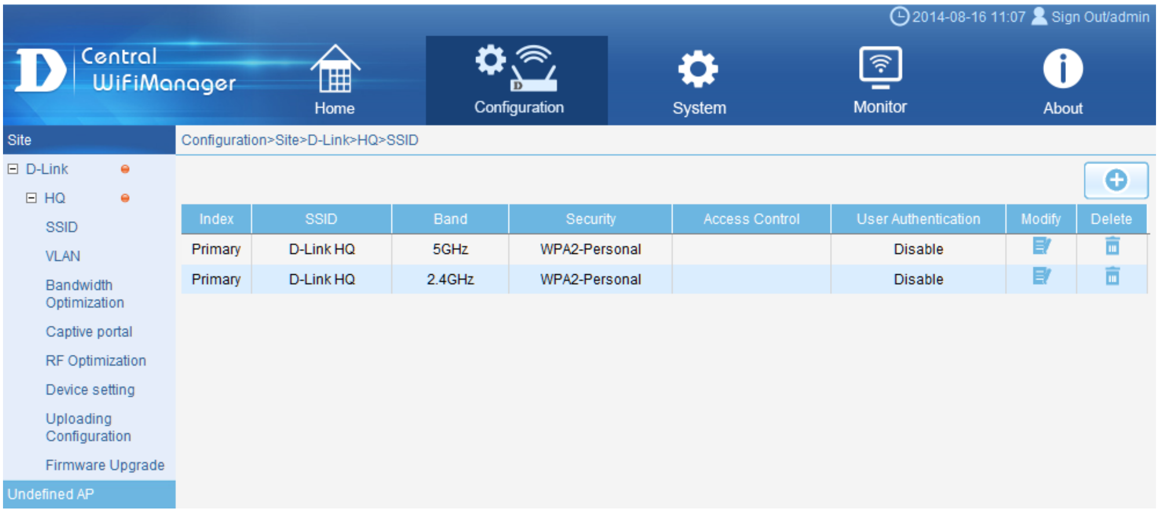
Figure 2-1 Captive Portal and User Authentication Network Layout

The overview of the configuration steps for Captive Portal is as follows:

1. Configure Captive Portal with Local Database Authentication
2. Configure Captive Portal with Passcode Authentication

2.1. Configure Captive Portal with Local Database Authentication

In this section we'll create a new guest SSID and configure this SSID to use the local database for authentication. To create a new SSID, navigate to **Configuration > Site** (D-Link) **> Network** (HQ).

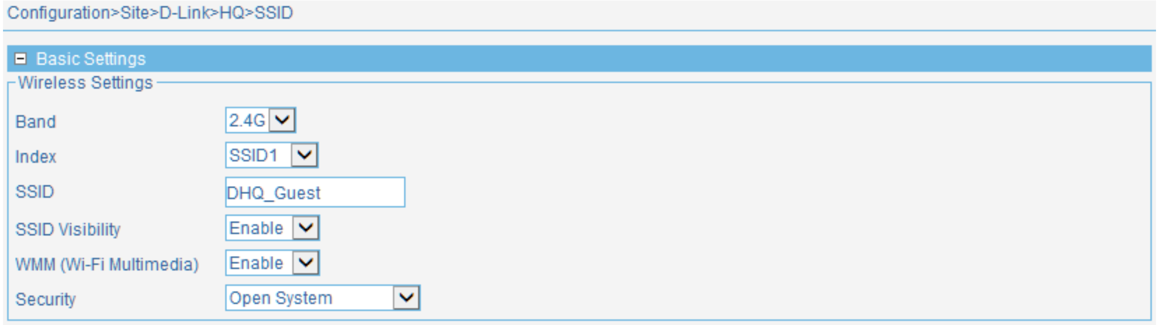


Configuration>Site>D-Link>HQ>SSID

Index	SSID	Band	Security	Access Control	User Authentication	Modify	Delete
Primary	D-Link HQ	5GHz	WPA2-Personal		Disable		
Primary	D-Link HQ	2.4GHz	WPA2-Personal		Disable		

Figure 2-2 Create Guest SSID (Local Database Authentication)

To create a new 2.4GHz guest **SSID** (DHQ_Guest), select the existing **Network** (HQ) and click the ⊕ button. Select the **Band** (2.4G), **Index** (SSID1), enter the **SSID** (DHQ_Guest), and configure the wireless security settings. In this example we used **Open System** for wireless security. Click **Save** to apply the settings.


Configuration>Site>D-Link>HQ>SSID

Basic Settings

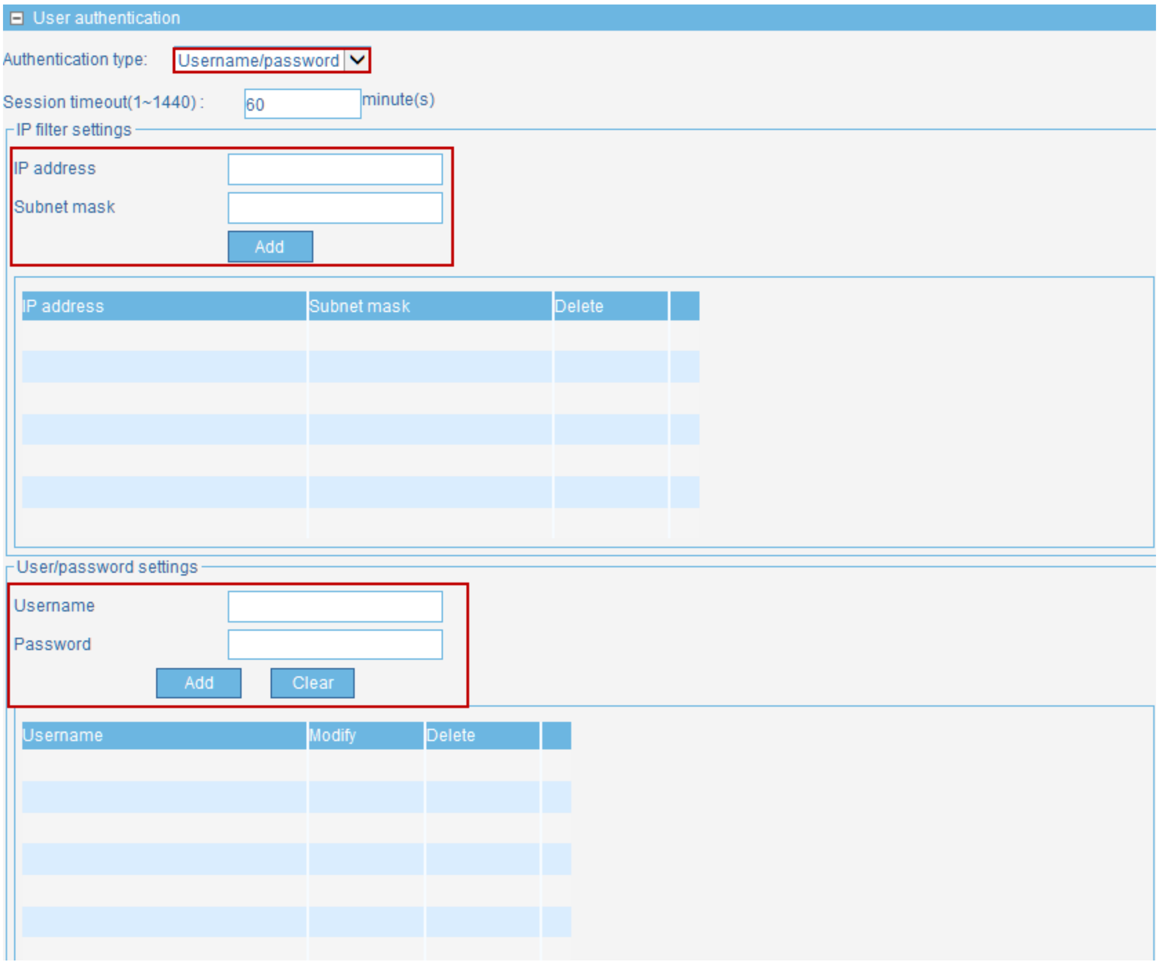
Wireless Settings

Band	2.4G
Index	SSID1
SSID	DHQ_Guest
SSID Visibility	Enable
WMM (Wi-Fi Multimedia)	Enable
Security	Open System

Figure 2-3 Configure Guest SSID

In **User Authentication** section, select **Username/Password**. To prevent guest users from accessing your intranet, enter the intranet's IP ranges in the **IP Filter setting** spaces provided. Enter the new guest account's **Username** and **Password** in the spaces provided. Click the **Add** button to add the new guest user account to the table.

NOTE. In default settings, IP filter function is disabled and all wireless clients can access all networks.

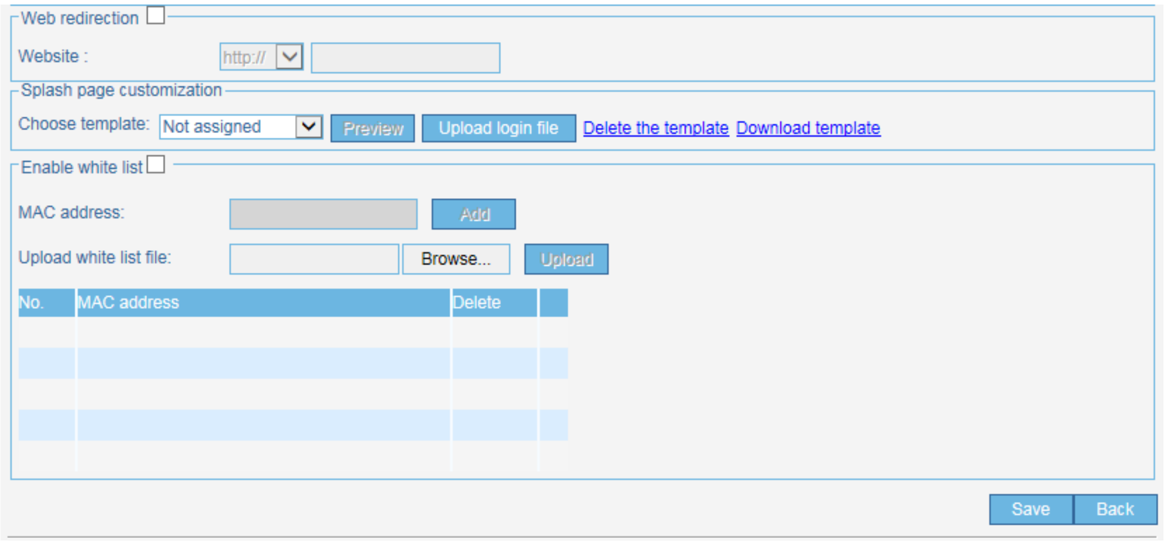


Authentication type: Username/password

Session timeout(1~1440) : 60 minute(s)

Figure 2-4 Configuration Guest SSID User Authentication

Select the **Web Redirection** option to enable web redirection. Enter a **Web Site** (www.google.com) in the space provided. In **Splash page customization section**, select the template of splash page.(For detail please refer to scenario 3) In the **White List** section, it allows to configure what network devices are permitted to connect to this network by specifying the MAC address of those network devices. Click the **Save** button to accept the changes made.



Web redirection □

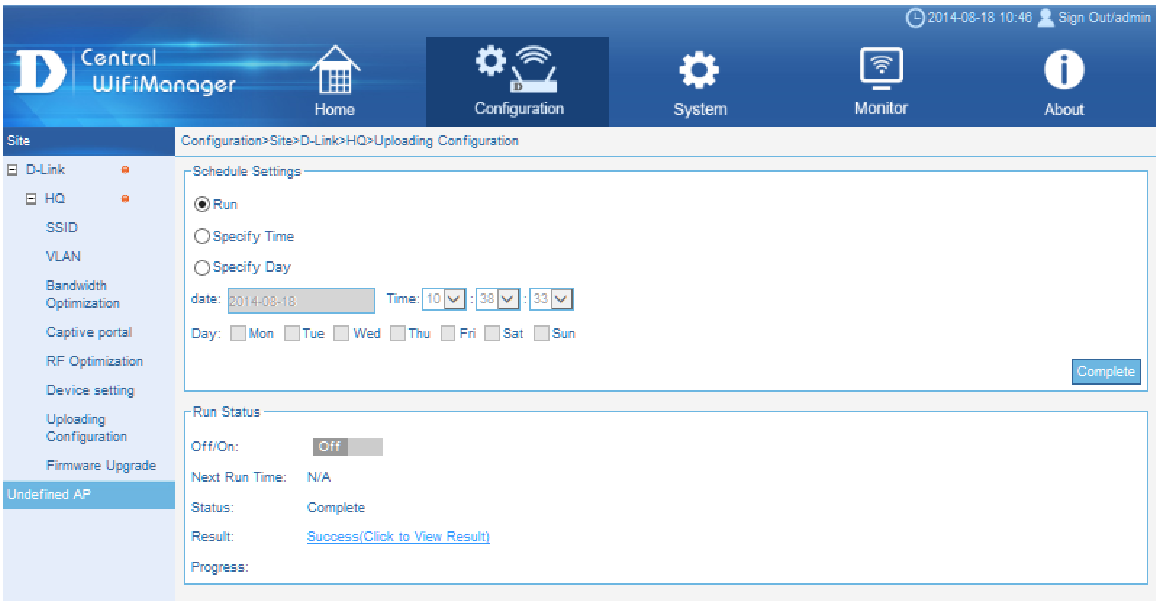
Website : http://

Choose template: Not assigned

Enable white list □

Figure 2-5 Captive Portal Settings

Navigate to **Configuration > Site** (D-Link) **> Network** (HQ) and select the **Upload Configuration** option in the left menu. Then select the **Run** option and click the **Complete** button to upload the modified settings to the access points associated with this network.



Configuration>Site>D-Link>HQ>Uploading Configuration

Schedule Settings

● Run

○ Specify Time

○ Specify Day

date: 2014-08-18 Time: 10 : 38 : 33

Day: □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Run Status

Off/On: Off

Next Run Time: N/A

Status: Complete

Result: Success(Click to View Result)

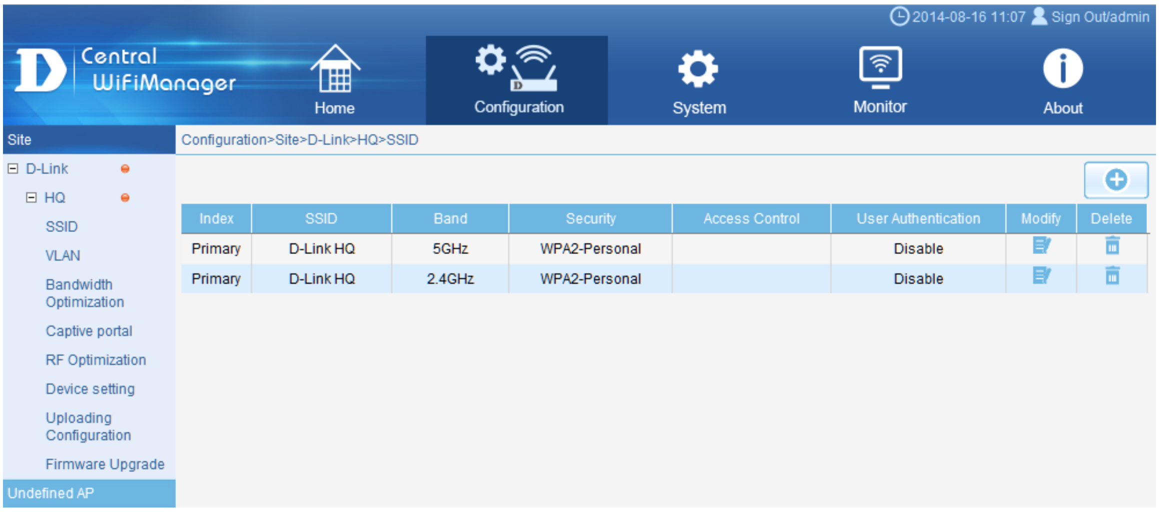
Progress:

Figure 2-6 Uploading Configuration

2.2. Configure Captive Portal with Passcode Authentication

2.2.1. Configure SSID for Passcode Authentication

In this section we'll create a new guest SSID and configure this SSID to use passcode authentication. To create a new SSID, navigate to **Configuration > Site** (D-Link) **> Network** (HQ).

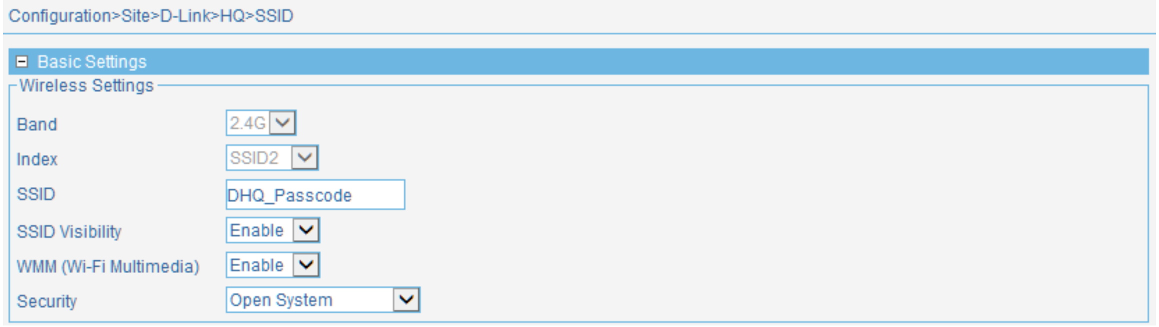


Configuration>Site>D-Link>HQ>SSID

Index	SSID	Band	Security	Access Control	User Authentication	Modify	Delete
Primary	D-Link HQ	5GHz	WPA2-Personal		Disable		
Primary	D-Link HQ	2.4GHz	WPA2-Personal		Disable		

Figure 2-7 Create Guest SSID (Passcode)

To create a new 2.4GHz guest **SSID** (DHQ_Passcode), select the existing **Network** (HQ) and click the ⊕ button. Select the **Band** (2.4G), **Index** (SSID2), enter the **SSID** (DHQ_Passcode), and configure the wireless security settings. In this example we used **Open System** for wireless security. Click **Save** to apply the settings.



Configuration>Site>D-Link>HQ>SSID

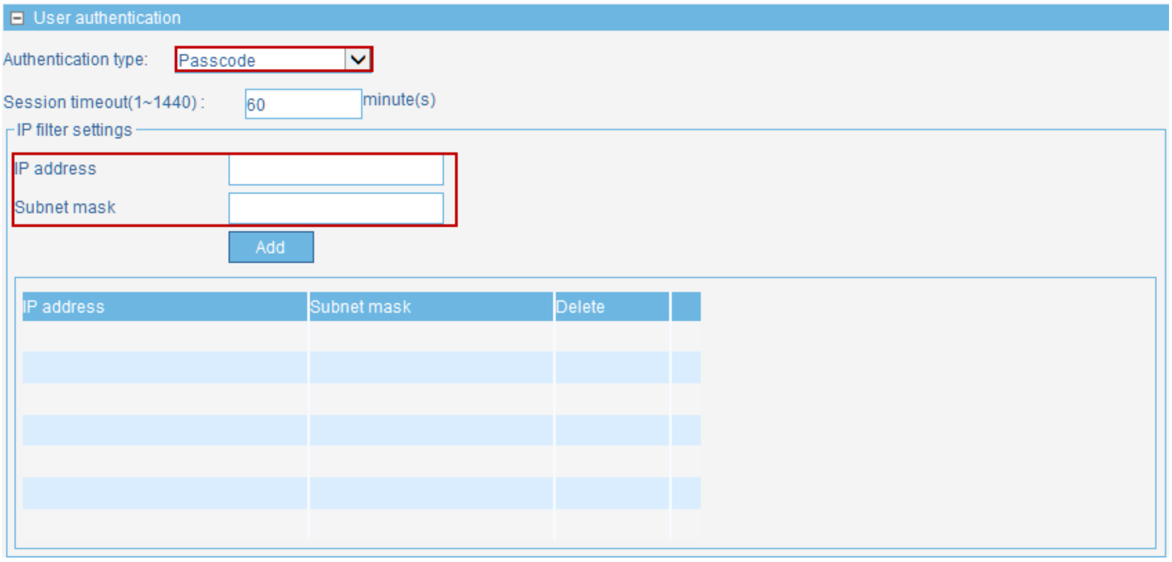
Basic Settings

Wireless Settings

Band	2.4G
Index	SSID2
SSID	DHQ_Passcode
SSID Visibility	Enable
WMM (Wi-Fi Multimedia)	Enable
Security	Open System

Figure 2-8 Configure Guest SSID (Passcode)

In **User Authentication** section, select **Passcode**. Click the **Save** button to accept the changes made. To prevent guest users from accessing your intranet, enter the intranet's IP ranges in the **IP Filter setting** spaces provided.



User authentication

Authentication type: Passcode

Session timeout(1~1440) : 60 minute(s)

IP filter settings

IP address

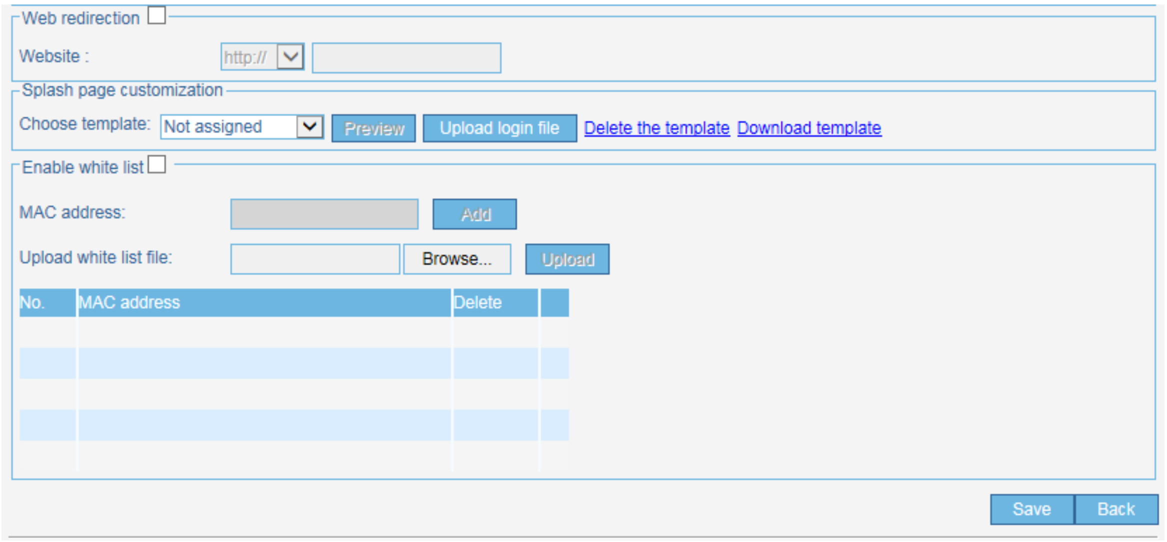
Subnet mask

Add

IP address	Subnet mask	Delete

Figure 2-9 User Authentication (Passcode)

Select the **Web Redirection** option to enable web redirection. Enter a **Web Site** (www.google.com) in the space provided. In **Splash page customization section**, select the template of splash page.(For detail please refer to scenario 3) In the **White List** section, it allows to configure what network devices are permitted to connect to this network by specifying the MAC address of those network devices. Click the **Save** button to accept the changes made.



Web redirection □

Website : http://

Splash page customization

Choose template: Not assigned

Preview | Upload login file | Delete the template | Download template

Enable white list □

MAC address: Add

Upload white list file: Browse... Upload

No.	MAC address	Delete

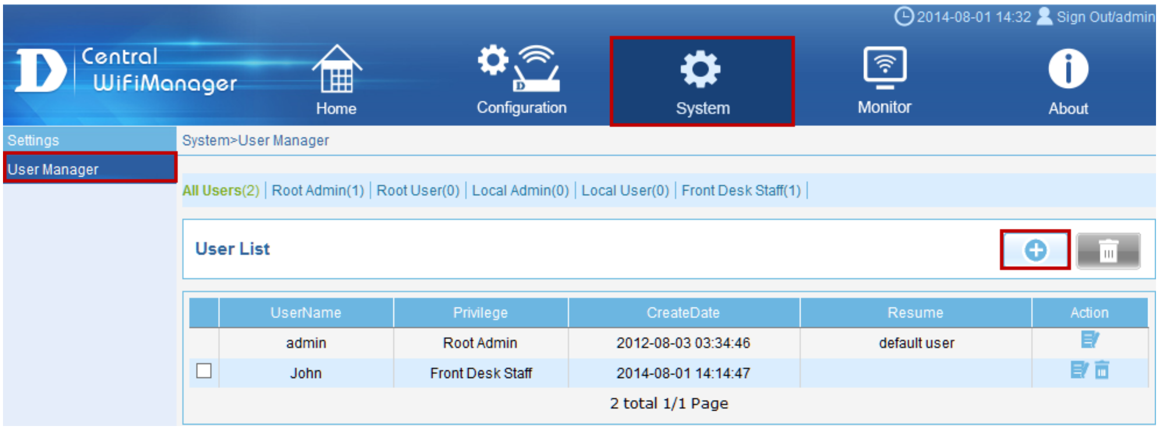
Save | Back

Figure 2-10 Captive Portal Settings

2.2.2. Create Front Desk Account

To create a new **Front Desk User Account** navigate to **System > User Manager** and click the ⊕ button.

NOTE. In current design, only the front desk account can create and delete the passcode



2014-08-01 14:32 Sign Out/admin

System>User Manager

All Users(2) | Root Admin(1) | Root User(0) | Local Admin(0) | Local User(0) | Front Desk Staff(1) |

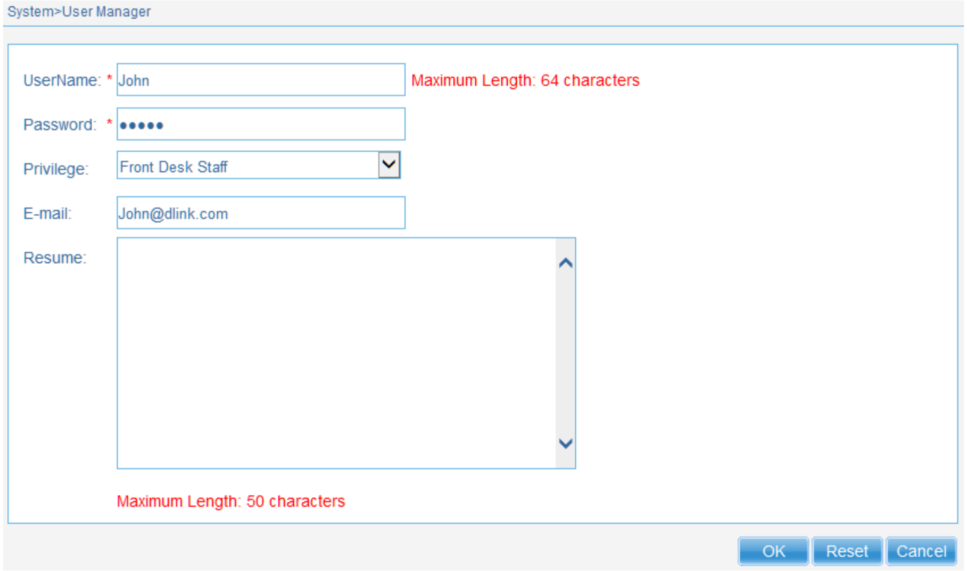
User List

	UserName	Privilege	CreateDate	Resume	Action
	admin	Root Admin	2012-08-03 03:34:46	default user	✎
□	John	Front Desk Staff	2014-08-01 14:14:47		✎ 🗑

2 total 1/1 Page

Figure 2-11 User Manager

Enter the **UserName** (John) and **Password** (1234) for this new account in the spaces provided. Select the **Front Desk Staff** option as the **Privilege** and enter the new account's **E-mail** address in the space provided. Click the **OK** button create the new user account.



System>User Manager

UserName: * John — Maximum Length: 64 characters

Password: * ●●●●●

Privilege: Front Desk Staff

E-mail: John@dlink.com

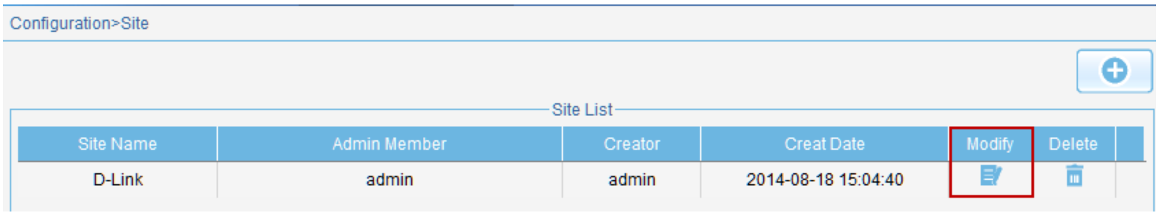
Resume:

Maximum Length: 50 characters

Figure 2-12 Create New Front Desk Account

2.2.3. Add the Front Desk Account to the Site and Network

To add the **Front Desk Account** to the site and network navigate to **Configuration > Site** (D-Link) and click the **Modify** icon (✎).



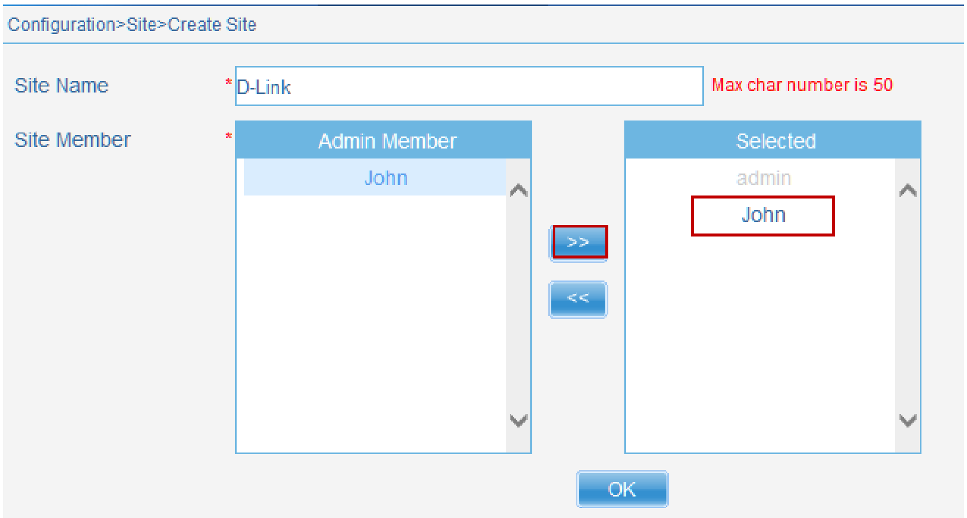
Configuration>Site

Site List

Site Name	Admin Member	Creator	Creat Date	Modify	Delete
D-Link	admin	admin	2014-08-18 15:04:40	✎	🗑

Figure 2-13 Add Front Desk Account to Site (Step 1)

After clicking the modify icon (✎), select the **Front Desk Account** and add it to the selected table by click the **>>** button. Click the **OK** button to accept the changes made.



Configuration>Site>Create Site

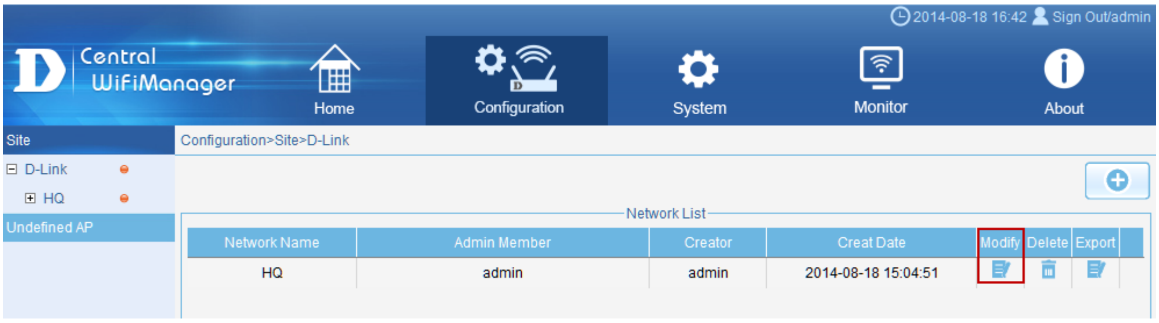
Site Name * D-Link Max char number is 50

Site Member *

Admin Member	Selected
John	admin John

Figure 2-14 Add Front Desk Account to Site (Step 2)

Navigate to **Configuration > Site** (D-Link) **> Network** (HQ) and click the **Modify** icon (✎).



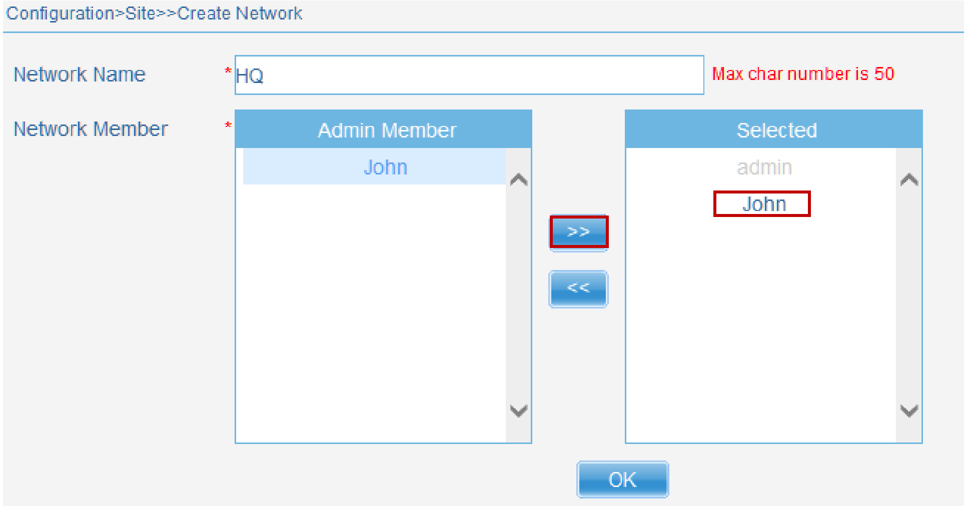
Configuration>Site>D-Link

Network List

Network Name	Admin Member	Creator	Creat Date	Modify	Delete	Export
HQ	admin	admin	2014-08-18 15:04:51	✎	🗑	✎

Figure 2-15 Add Front Desk Account to Network (Step 1)

After clicking the modify icon (✎), select the **Front Desk Account** and add it to the selected table by click the **>>** button. Click the **OK** button to accept the changes made.



Configuration>Site>>Create Network

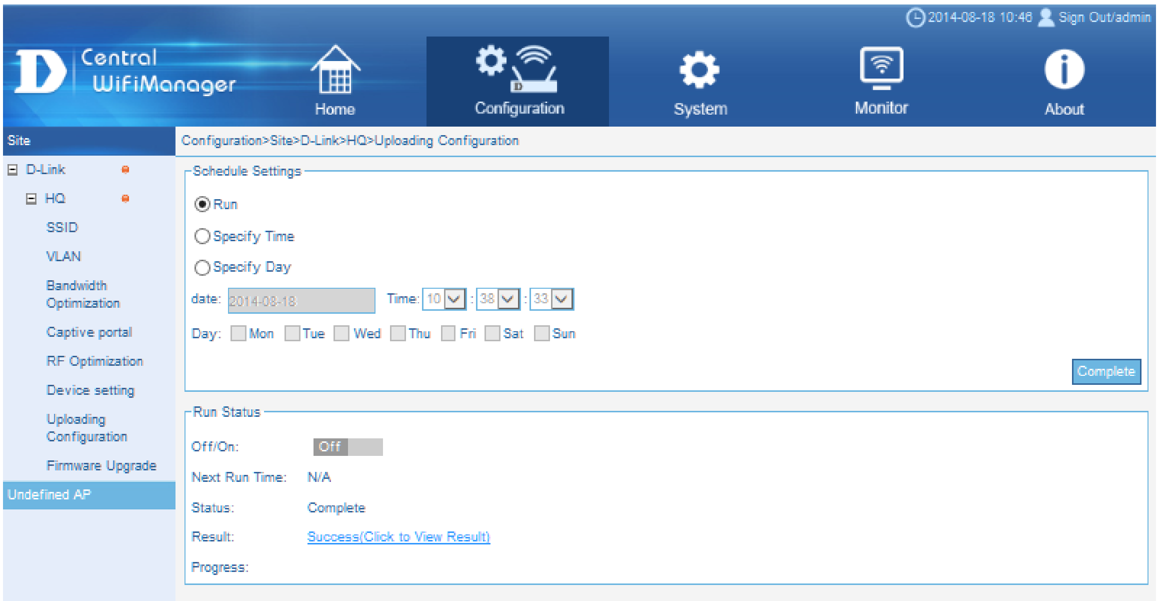
Network Name * HQ Max char number is 50

Network Member *

Admin Member	Selected
John	admin John

Figure 2-16 Add Front Desk Account to Network (Step 2)

Navigate to **Configuration > Site** (D-Link) **> Network** (HQ) and select the **Upload Configuration** option in the left menu. Then select the **Run** option and click the **Complete** button to upload the modified settings to the access points associated with this network.



Configuration>Site>D-Link>HQ>Uploading Configuration

Schedule Settings

● Run

○ Specify Time

○ Specify Day

date: 2014-08-18 Time: 10 : 38 : 33

Day: □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Complete

Run Status

Off/On: Off

Next Run Time: N/A

Status: Complete

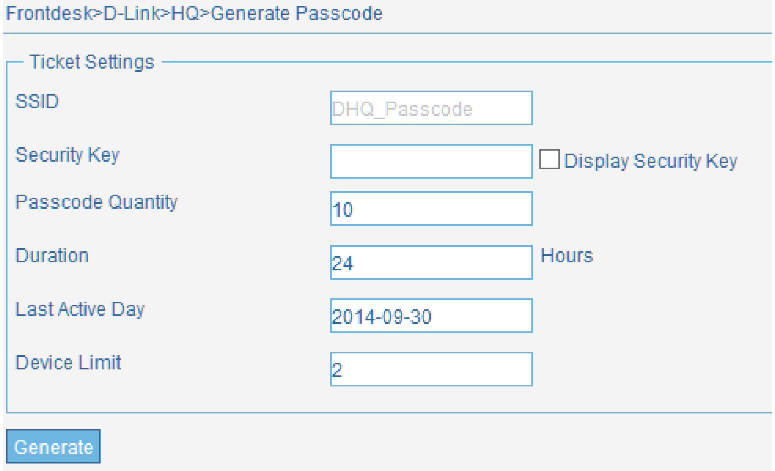
Result: Success(Click to View Result)

Progress:

Figure 2-17 Uploading Configuration

2.2.4. Generate Passcode to Guest

To generate a **Passcode** for the **Front Desk Account**, we need to logout of the CWM and then log back into the CWM using the Front Desk Account's username and password. After logging back in, enter the **Passcode Quantity** (10), **Duration** (24) and **Device Limit** (2) information in the spaces provided; and click the **Generate** button.


Frontdesk>D-Link>HQ>Generate Passcode

Ticket Settings

SSID: DHQ_Passcode

Security Key: □ Display Security Key

Passcode Quantity: 10

Duration: 24 Hours

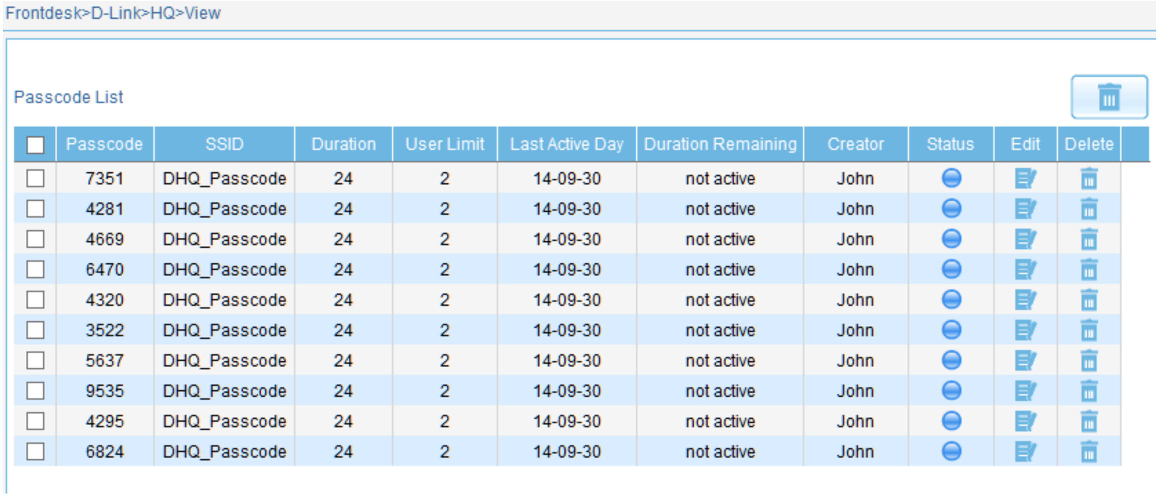
Last Active Day: 2014-09-30

Device Limit: 2

Generate

Figure 2-18 Generate Passcode

On the **View** page, a list of generated passcodes for this front desk account will be displayed.



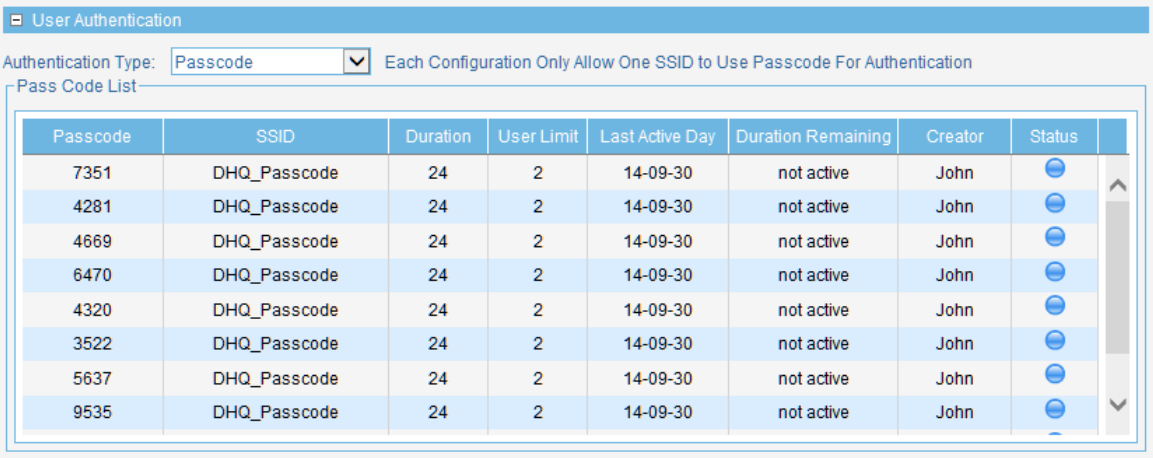
Frontdesk>D-Link>HQ>View

Passcode List

□	Passcode	SSID	Duration	User Limit	Last Active Day	Duration Remaining	Creator	Status	Edit	Delete
□	7351	DHQ_Passcode	24	2	14-09-30	not active	John	●	✎	🗑
□	4281	DHQ_Passcode	24	2	14-09-30	not active	John	●	✎	🗑
□	4669	DHQ_Passcode	24	2	14-09-30	not active	John	●	✎	🗑
□	6470	DHQ_Passcode	24	2	14-09-30	not active	John	●	✎	🗑
□	4320	DHQ_Passcode	24	2	14-09-30	not active	John	●	✎	🗑
□	3522	DHQ_Passcode	24	2	14-09-30	not active	John	●	✎	🗑
□	5637	DHQ_Passcode	24	2	14-09-30	not active	John	●	✎	🗑
□	9535	DHQ_Passcode	24	2	14-09-30	not active	John	●	✎	🗑
□	4295	DHQ_Passcode	24	2	14-09-30	not active	John	●	✎	🗑
□	6824	DHQ_Passcode	24	2	14-09-30	not active	John	●	✎	🗑

Figure 2-19 Display Passcodes (Front Desk Account)

Administrators can also view the passcode list when logged back into the CWM as administrator. To view the passcode list as administrator, navigate to **Configuration > Site** (D-Link) **> Network** (HQ) **>SSID** (DHQ_Passcode). Click the **Modify** icon (✎) and in the **User Authentication** section the list of passcodes will be displayed.



⊟ User Authentication

Authentication Type: Passcode ▾ Each Configuration Only Allow One SSID to Use Passcode For Authentication

Pass Code List

Passcode	SSID	Duration	User Limit	Last Active Day	Duration Remaining	Creator	Status
7351	DHQ_Passcode	24	2	14-09-30	not active	John	●
4281	DHQ_Passcode	24	2	14-09-30	not active	John	●
4669	DHQ_Passcode	24	2	14-09-30	not active	John	●
6470	DHQ_Passcode	24	2	14-09-30	not active	John	●
4320	DHQ_Passcode	24	2	14-09-30	not active	John	●
3522	DHQ_Passcode	24	2	14-09-30	not active	John	●
5637	DHQ_Passcode	24	2	14-09-30	not active	John	●
9535	DHQ_Passcode	24	2	14-09-30	not active	John	●

Figure 2-20 Display Passcodes (Administrator Account)

Scenario 3 - Customize Captive Portal Login Page

There are three styling options provided for customizing the look and feel of the captive portal login page. Please follow instructions below for a successful customization of the login page.

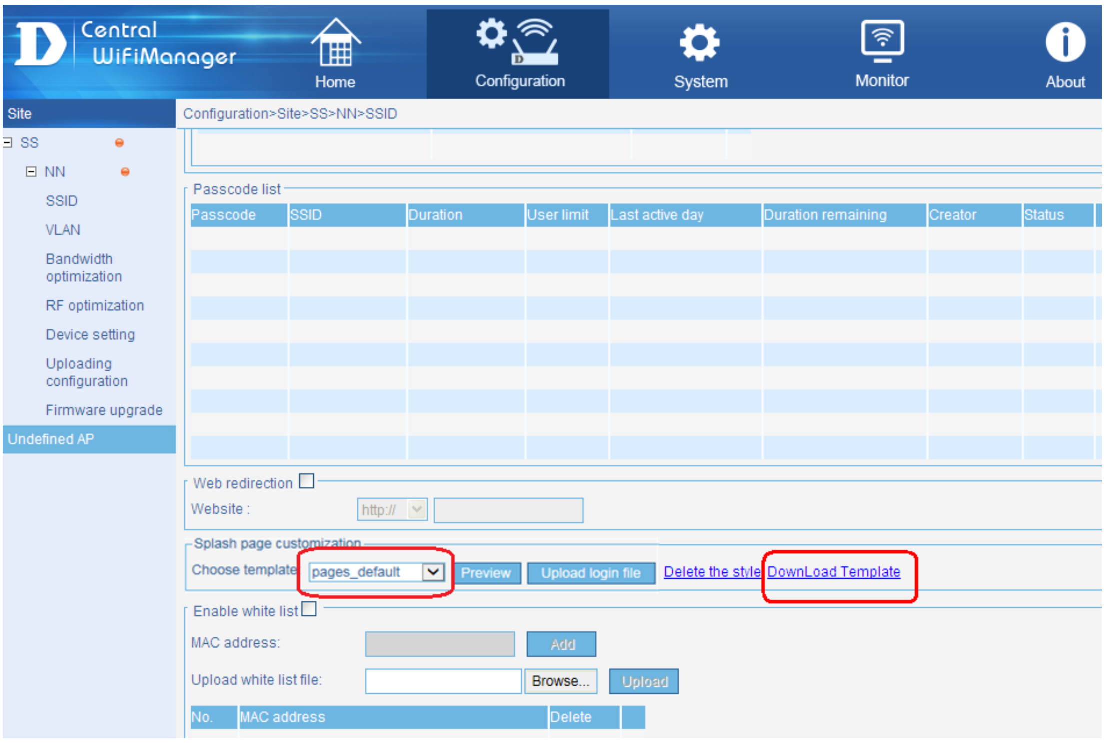
Each styling option represents different UI style; customization for any option is done by editing its web page source files. Below is a quick overview for files that can be edited as they vary for each styling option:

- Pages default: Provides options to customize the text and images shown on the login page
- Pages license: Provides options to customize the text and images shown on the login page, including the ability to place your own logo image.
- Pages_headerpic: Provides options to customize the text and images shown on the login page, including the ability to place your own logo image and a header image at the top of the page.

Image is customized by replacing the existing image files. Text is customized by editing the “text.js” file.

3.1. Obtaining the source files

You can obtain the source file by going to the “SSID” page under the “Configuration” menu. In “Splash page customization”, select the style from the drop-down menu and click on “Download Template” to download its source file.



Configuration>Site>SS>NN>SSID

Passcode	SSID	Duration	User limit	Last active day	Duration remaining	Creator	Status

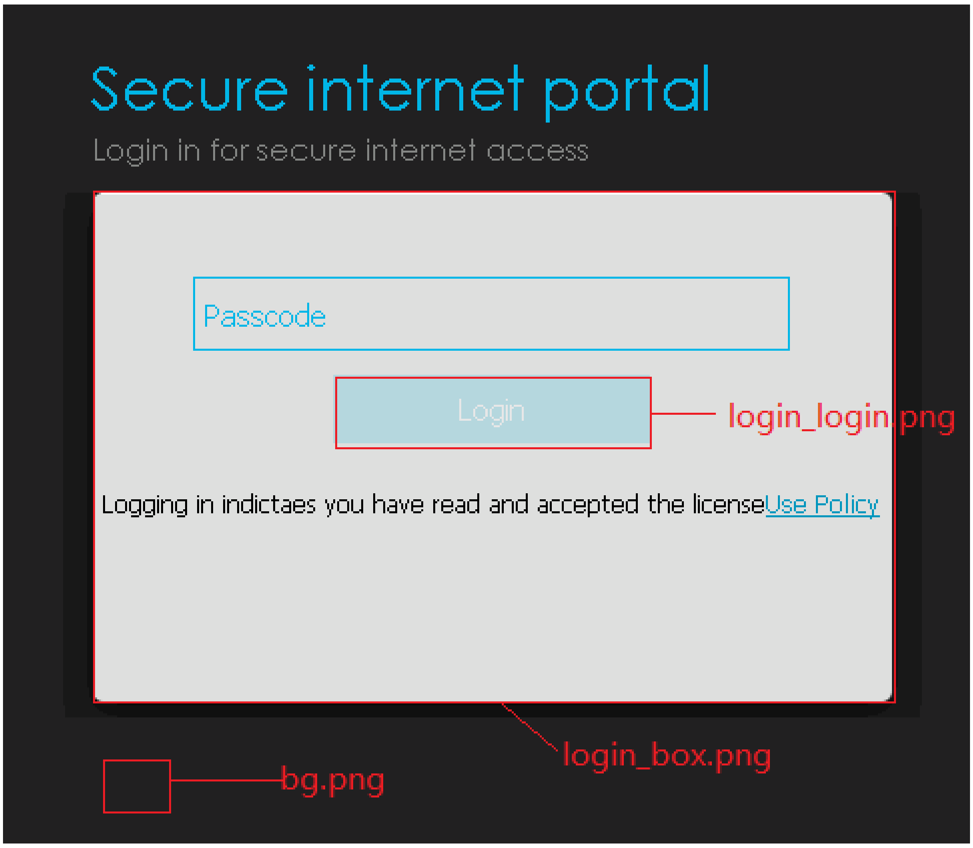
Choose template: pages_default

No.	MAC address	Delete

You should see the downloaded source file with the same name as the one from the drop-down menu. The file will be compressed with the extension of “.tar” (eg. Pages_default.tar). Please use a file compression tool such as 7zip or winrar to decompress the file. The source files should then be located in an extracted folder.

3.2. Contents and illustrations of each styling source files

- **Pages_default:** bg.png, login_box.png, login_login.png, text.js
  - *Please make sure to use png image files and remain using the same file names for your customization.*
  - *Please make sure UTF-8 encoding for texts entered in the text.js file.*



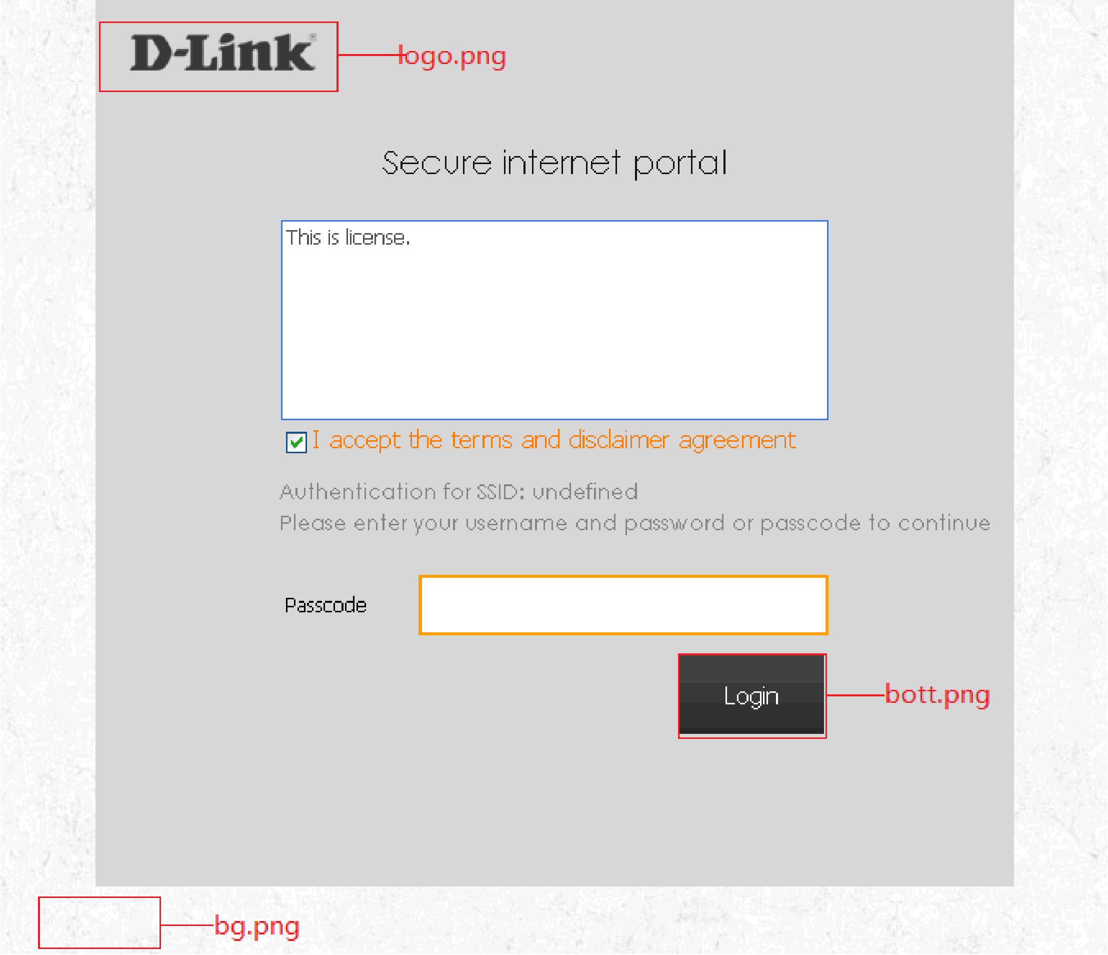
Secure internet portal

Login in for secure internet access

Passcode

Logging in indictaes you have read and accepted the licenseUse Policy

- **Pages_license:** bg.png, bott.png, logo.png, text.js
  - *Please make sure to use png image files and remain using the same file names for your customization.*
  - *Please make sure UTF-8 encoding for texts entered in the text.js file.*



Secure internet portal

This is license.

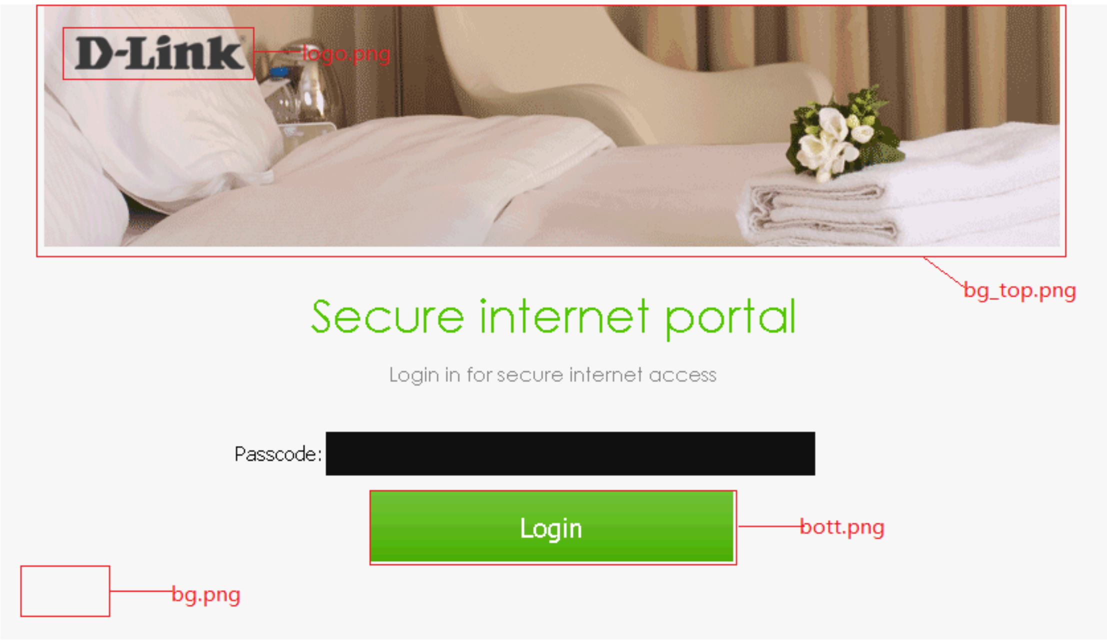
☑ I accept the terms and disclaimer agreement

Authentication for SSID: undefined

Please enter your username and password or passcode to continue

Passcode

- **Pages_headerpic:** bg.png, bg_top.png, bott.png, logo.png, text.js
    - *Please make sure to use png image files and remain using the same file names for your customization.*
    - *Please make sure UTF-8 encoding for texts entered in the text.js file.*



3.3. Editing texts in the text.js file

Open the text.js with text editor software. Locate the following parameters in the file and change their values to after the “=” to customize texts shown in the login page:

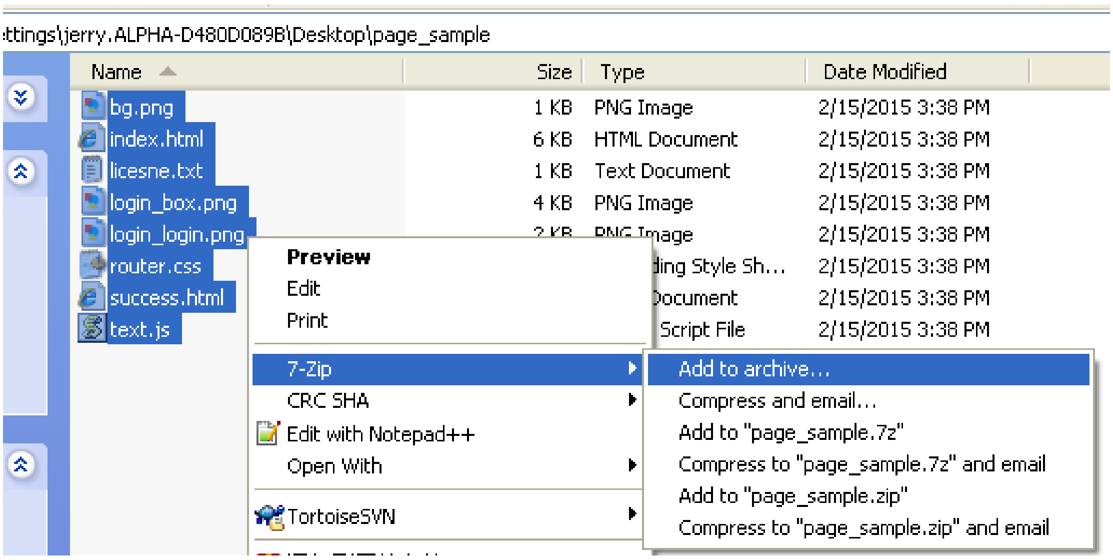
```
var username="Username";
var password="Password";
var login="Login";
var license_notice="Logging in indicates you have read and accepted the license";
var license_link="Use Policy";
```

3.4. Uploading the source file after customization

After you are done editing the extracted source files, you would need to compress the files back to a “.tar” file before uploading it back the CWM.

Below is an example to compress the files using 7zip:

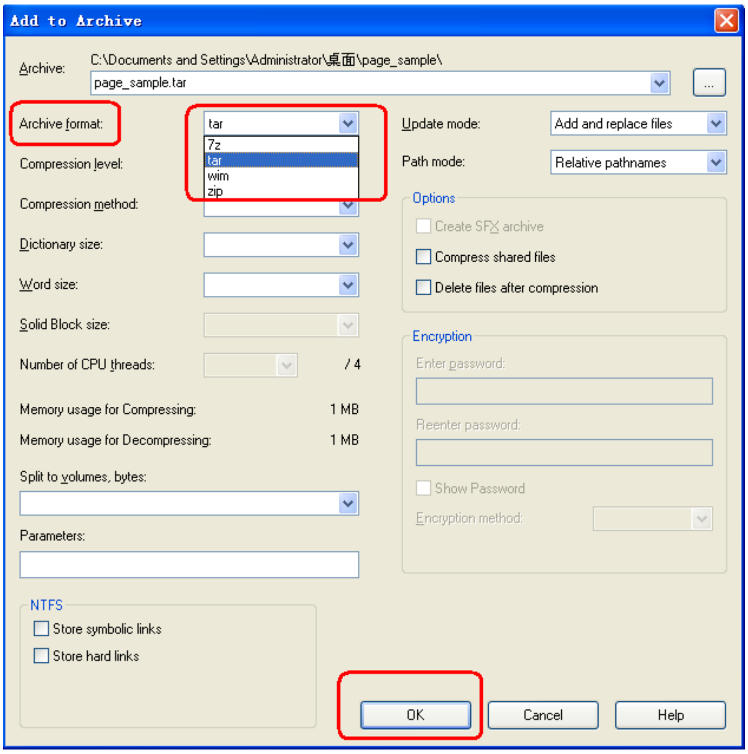
1. Select all the extracted source files and right-click. From the drop-down menu, select “7-Zip” >> “Add to archive”



ttings\jerry.ALPHA-D480D089B\Desktop\page_sample

Name	Size	Type	Date Modified
bg.png	1 KB	PNG Image	2/15/2015 3:38 PM
index.html	6 KB	HTML Document	2/15/2015 3:38 PM
licesne.txt	1 KB	Text Document	2/15/2015 3:38 PM
login_box.png	4 KB	PNG Image	2/15/2015 3:38 PM
login_login.png	2 KB	PNG Image	2/15/2015 3:38 PM
router.css		ding Style Sh...	2/15/2015 3:38 PM
success.html		ocument	2/15/2015 3:38 PM
text.js		Script File	2/15/2015 3:38 PM

2. In the dialog, select “tar” as the archive format from the drop-down menu shown below and click “OK” to finish. *(*Please make sure the compressed file does not exceed 448KB. Exceeding the size limit will result in a failed upload)*



Add to Archive

Archive: C:\Documents and Settings\Administrator\桌面\page_sample\
page_sample.tar

Archive format: tar

Update mode: Add and replace files

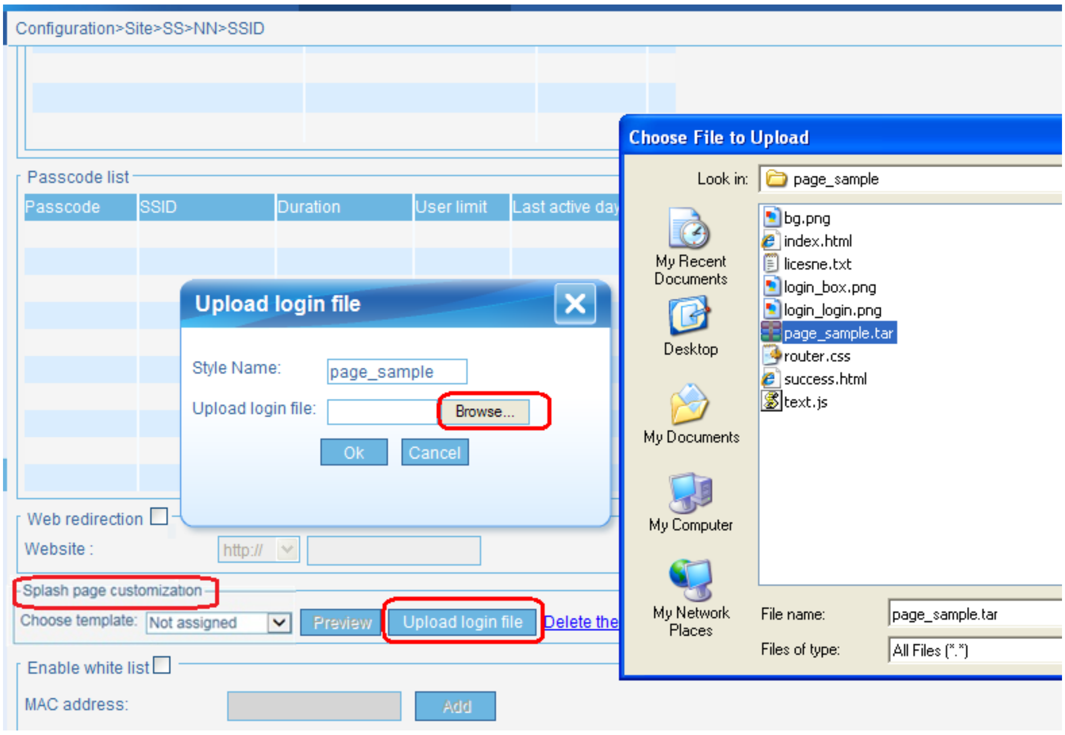
Path mode: Relative pathnames

Number of CPU threads: / 4

Memory usage for Compressing: 1 MB

Memory usage for Decompressing: 1 MB

3. In the CWM web management UI, go to “Configuration” >> “SSID”. Under “Splash page customization”, click “Upload login file”.   A dialog should be displayed to allow you to add a new style profile. Enter a desired name and click “Browse”, this should open another dialog which allows you to locate the source file for upload.



Configuration>Site>SS>NN>SSID

Upload login file

Style Name: page_sample

Upload login file:

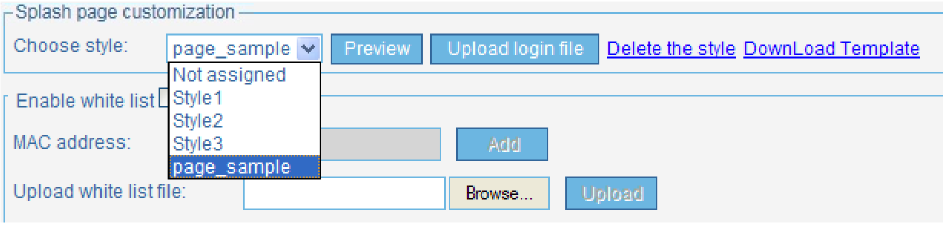
Choose File to Upload

Look in: page_sample

File name: page_sample.tar

Files of type: All Files (*.*)

4. After uploading the source file successfully, the new style should be available from the drop-down menu, which you can select and finish configuration for captive portal login page customization.



Splash page customization

Choose style: page_sample

Scenario 4 - Bandwidth Optimization

Bandwidth optimization allows administrators to control the wireless bandwidth usage. The **Downlink** and **Uplink Bandwidth** options allows for the limiting of the total bandwidth of access points. For more information about the various bandwidth optimization rules available in the CWM, refer to the *Central WiFiManager User Manual*.

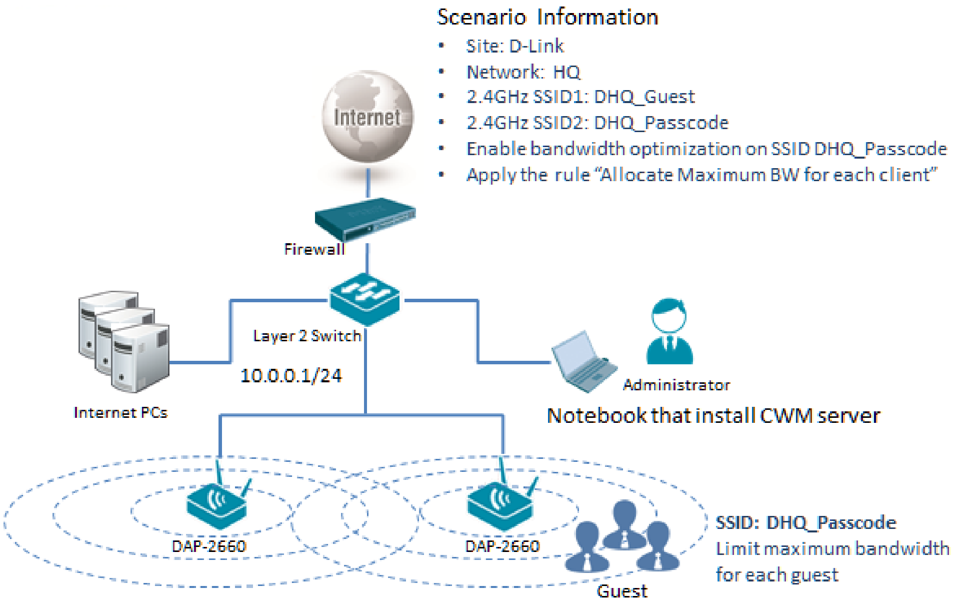
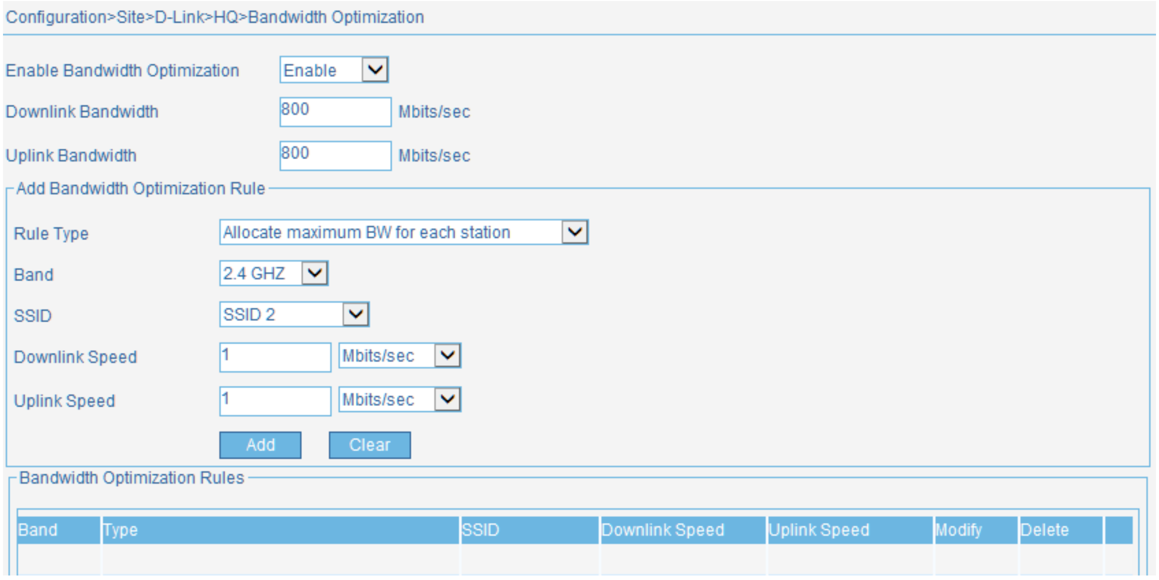

Scenario Information
• Site: D-Link
• Network: HQ
• 2.4GHz SSID1: DHQ_Guest
• 2.4GHz SSID2: DHQ_Passcode
• Enable bandwidth optimization on SSID DHQ_Passcode
• Apply the rule "Allocate Maximum BW for each client"
Internet
Firewall
Layer 2 Switch
10.0.0.1/24
Internet PCs
Administrator
Notebook that install CWM server
DAP-2660
DAP-2660
Guest
SSID: DHQ_Passcode
Limit maximum bandwidth
for each guest

Figure 4-1 Bandwidth Optimization Network Layout

4.1. Configure Bandwidth Optimization

To configure the Bandwidth Optimization settings, navigate to **Configuration > Site** (D-Link) **> Network** (HQ) **> Bandwidth Optimization**. At **Enable Bandwidth Optimization** select **Enable**. In the **Downlink Bandwidth** and **Uplink Bandwidth** fields enter 800Mbps. This is the bandwidth for whole AP. Select the **Rule Type** option called **Allocate maximum BW for each station**. Then select **2.4GHz** as the **Band**, and **SSID2** (DHQ_Passcode) as the **SSID**. In the **Downlink Speed** and **Uplink Speed** fields enter **1Mbits/sec**. Click the **Add** button to create the new rule and then click the **Save** button to accept the changes made.



Configuration>Site>D-Link>HQ>Bandwidth Optimization

Enable Bandwidth Optimization: Enable

Downlink Bandwidth: 800 Mbits/sec

Uplink Bandwidth: 800 Mbits/sec

Add Bandwidth Optimization Rule

Rule Type: Allocate maximum BW for each station

Band: 2.4 GHZ

SSID: SSID 2

Downlink Speed: 1 Mbits/sec

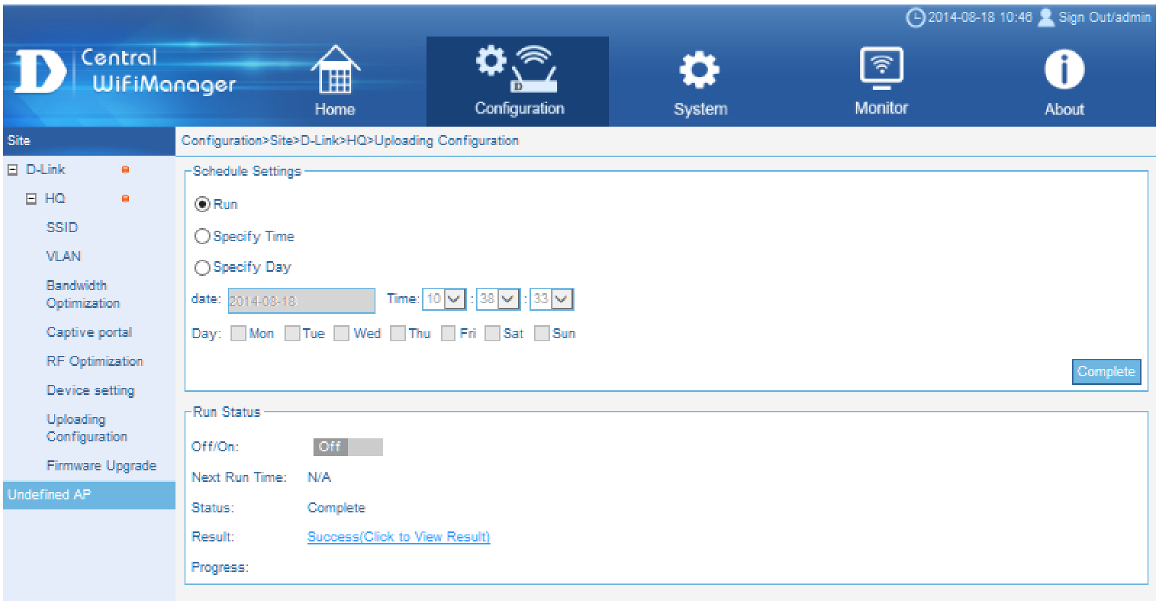
Uplink Speed: 1 Mbits/sec

Bandwidth Optimization Rules

Band	Type	SSID	Downlink Speed	Uplink Speed	Modify	Delete

Figure 4-2 Bandwidth Optimization Settings

Navigate to **Configuration > Site** (D-Link) **> Network** (HQ) and select the **Upload Configuration** option in the left menu. Then select the **Run** option and click the **Complete** button to upload the modified settings to the access points associated with this network.



Configuration>Site>D-Link>HQ>Uploading Configuration

Schedule Settings

● Run

○ Specify Time

○ Specify Day

date: 2014-08-18 Time: 10 : 38 : 33

Day: □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

Run Status

Off/On: Off

Next Run Time: N/A

Status: Complete

Result: Success(Click to View Result)

Progress:

Figure 4-3 Uploading Configuration

Scenario 5 - Add Remote AP for CWM Management

The CWM can manage remote access points over a site-to-site VPN or behind a NAT router without a VPN connection.

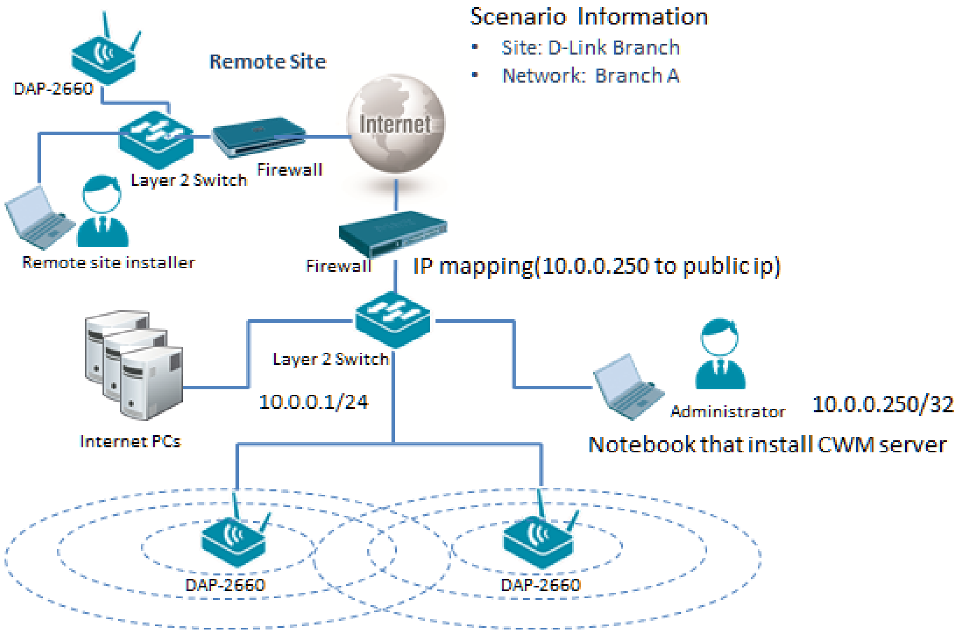


Figure 5-1 Remote AP for CWM Management Network Layout

The overview of the configuration steps for this configuration is as follows:

1. Configure Network Device Settings
2. Create New Site and Network for Branch Office
3. Export Network Profile then Import the Profile to the Remote AP

5.1. Configure Network Device Settings

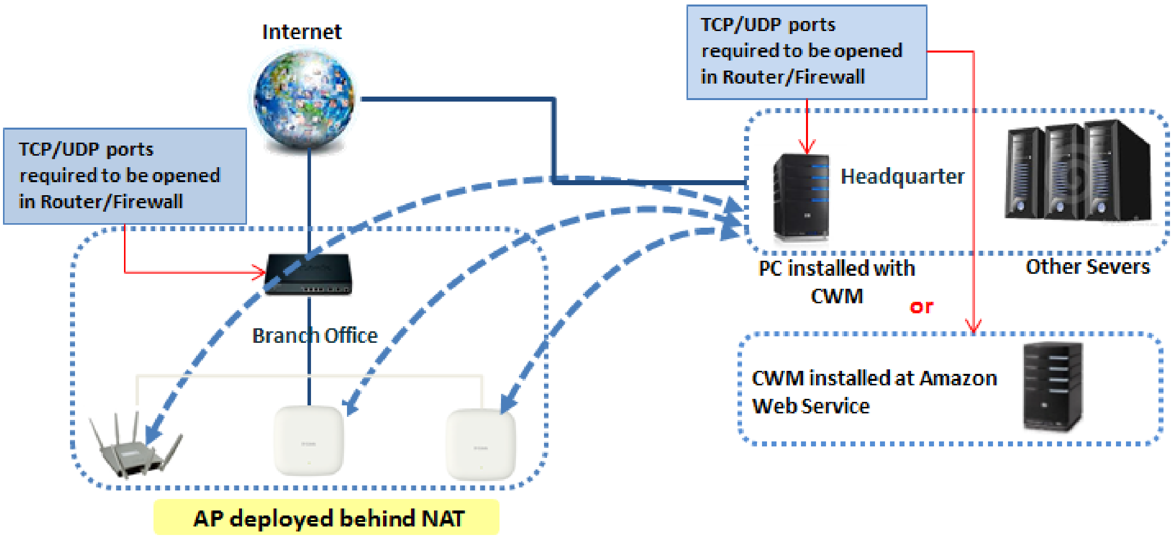
The following port numbers must be opened to allow inbound traffic in the firewall at the site where the CWM server is located in order for remote access points to access the CWM server.

- UDP 161 (SNMP port)
- UDP 162 (SNMP trap port)
- UDP 514 (Syslog port)
- UDP 8090 (Listen port)
- UDP 64768 (Service port)
- TCP 9000, enable ftp-ALG, **or** TCP 9000, TCP 10000 to 11000(Manager port) *
- TCP 443 (HTTPS, Management port)

Additionally, if the CWM server uses a private IP address, the public IP address must be mapped to the private IP address on the firewall.

At remote site, the following outbound ports also need to be opened.

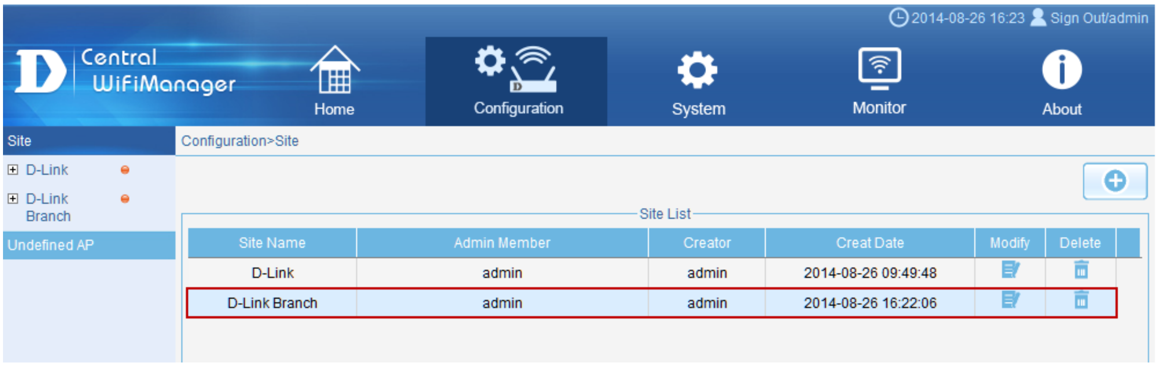
- UDP 161 (SNMP port)
- UDP 162 (SNMP trap port)
- UDP 514 (Syslog port)
- UDP 8090 (Listen port)
- UDP 64768 (Service port)
- TCP 9000, enable ftp-ALG, **or** TCP 9000, TCP 10000 to 11000(Manager port) *


Internet
TCP/UDP ports required to be opened in Router/Firewall
TCP/UDP ports required to be opened in Router/Firewall
Headquarter
PC installed with CWM
Other Severs
or
CWM installed at Amazon Web Service
Branch Office
AP deployed behind NAT

* In CWM v1.02, the ftp-ALG port is limited to TCP 10000 to 11000, if the CWM server is installed behind a firewall or an NAT device that does not support ftp-ALG, open TCP 9000, TCP 10000 to 11000 must be configured in order for the remote management to work properly.

5.2. Create New Site and Network for Branch Office

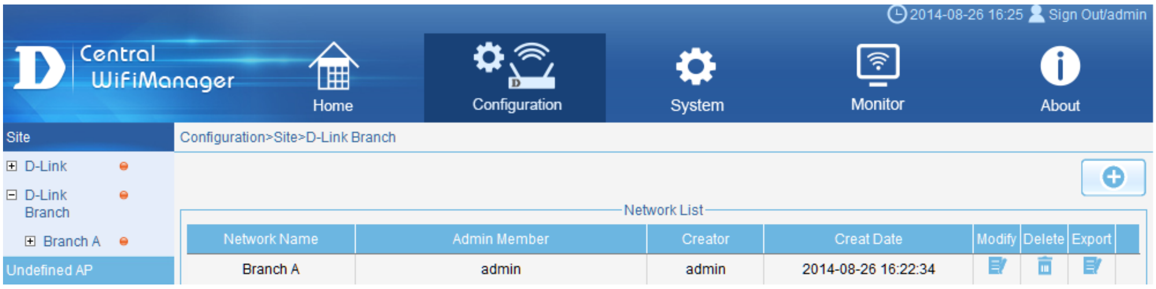
To create a new **Site** (D-Link Branch), select **Configuration** and then click the ⊕ button.



Site Name	Admin Member	Creator	Creat Date	Modify	Delete
D-Link	admin	admin	2014-08-26 09:49:48	✎	🗑
D-Link Branch	admin	admin	2014-08-26 16:22:06	✎	🗑

Figure 5-2 Create New Site (D-Link Branch)

To create a new **Network** (Branch-A), select the newly created **Site** (D-Link Branch) and click the ⊕ button.

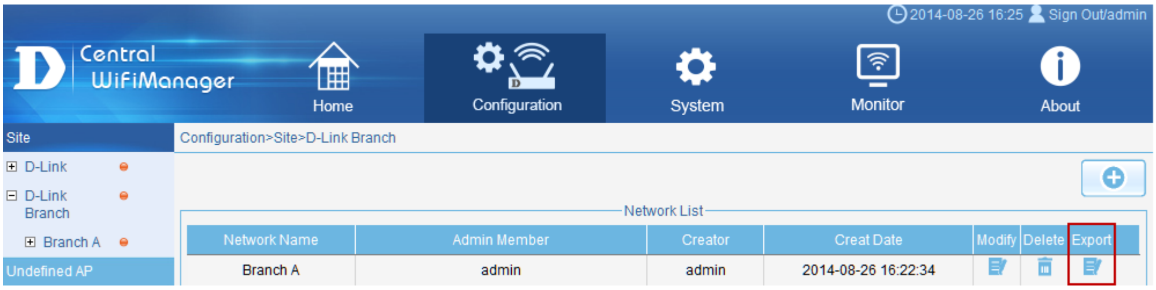


Network Name	Admin Member	Creator	Creat Date	Modify	Delete	Export
Branch A	admin	admin	2014-08-26 16:22:34	✎	🗑	✎

Figure 5-3 Create New Network (Branch-A)

5.3. Export Network Profile then Import the Profile to the Remote AP

To export the network profile select **Configuration > Site** (D-Link Branch) and then click the **Export** (✎) icon to export the network profile to your computer. Provide this exported network profile file to the remote site installer.

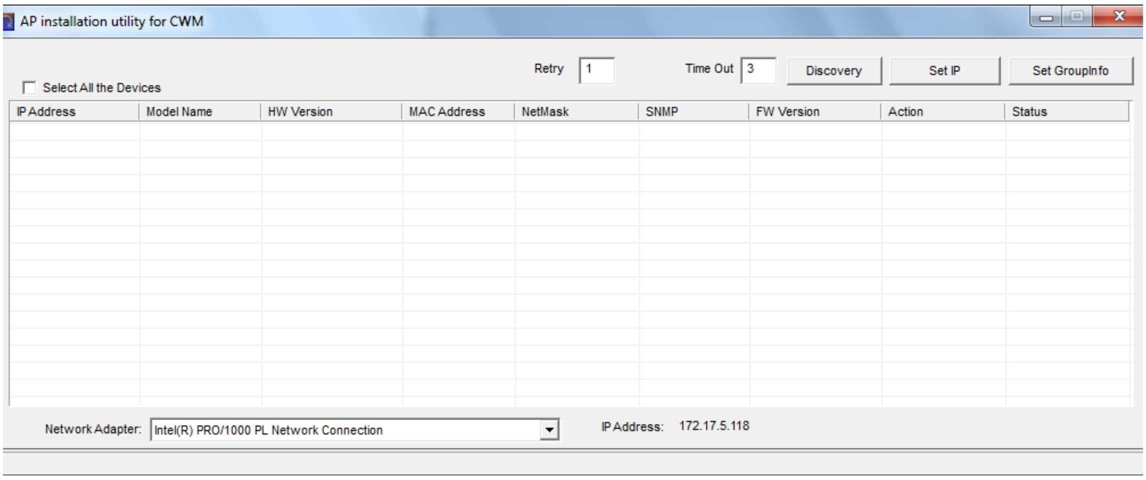


Network Name	Admin Member	Creator	Creat Date	Modify	Delete	Export
Branch A	admin	admin	2014-08-26 16:22:34	✎	🗑	✎

Figure 5-4 Export Network Profile to PC

At remote site, ensure that the exported network profile file is available on the computer used to configure the access point(s). Run the **Access Point Installation Utility for CWM**.

After opening the Access Point Installation Tool, the following window will be available. Click the **Discovery** button, to scan for D-Link access points that are connected to the network with an Ethernet cable.



Retry 1 Time Out 3

□ Select All the Devices

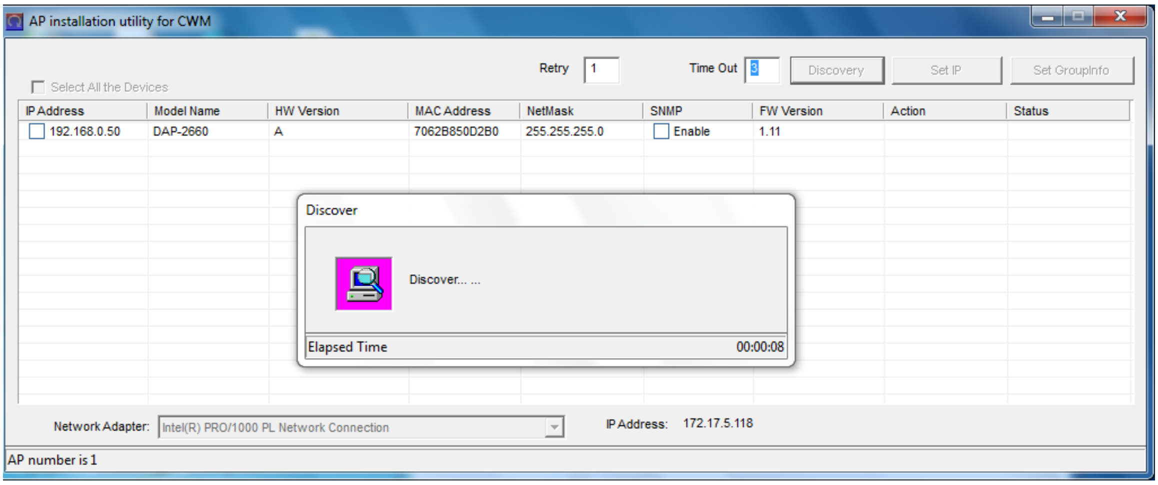
IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status

Network Adapter: Intel(R) PRO/1000 PL Network Connection

IP Address: 172.17.5.118

Figure 5-5 AP Installation Utility for CWM (Open)

After clicking the **Discovery** button, this utility will scan the LAN (Layer 2) network for D-Link access points that are connected to the network with an Ethernet cable.



Retry 1 Time Out 1

□ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
□ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	□ Enable	1.11		

Discover... ...

Elapsed Time 00:00:08

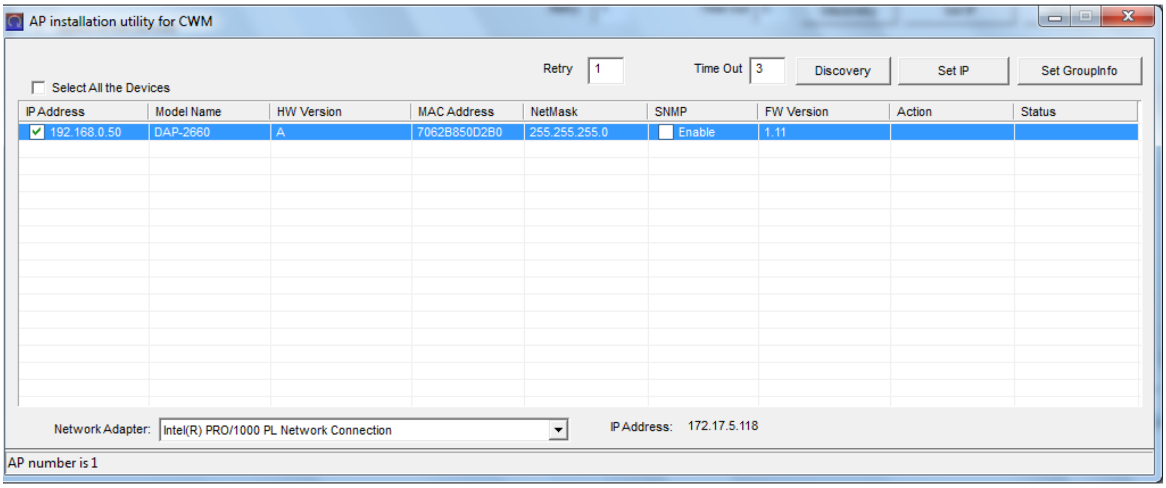
Network Adapter: Intel(R) PRO/1000 PL Network Connection

IP Address: 172.17.5.118

AP number is 1

Figure 5-6 AP Installation Utility for CWM (Discover)

After this utility found access point, they will be displayed and can be configured.



Retry 1 Time Out 3

□ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
☑ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	□ Enable	1.11		

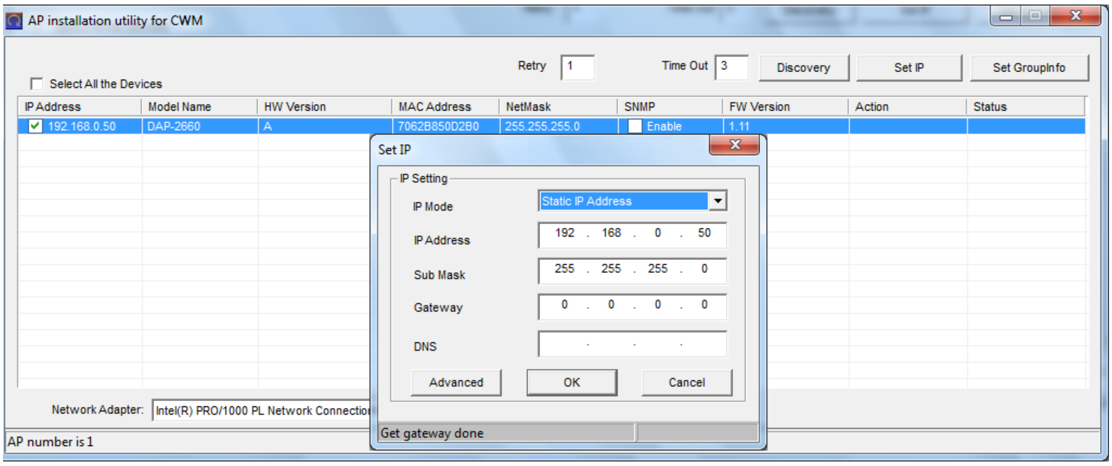
Network Adapter: Intel(R) PRO/1000 PL Network Connection

IP Address: 172.17.5.118

AP number is 1

Figure 5-7 AP Installation Utility for CWM (Found)

To modify the IP address of the newly discovered access point, select it and click the **Set IP** button. Enter the new IP address, subnet mask, gateway address and primary DNS address in the spaces provided. Click **OK** to accept the changes made.



AP installation utility for CWM

Retry: 1 Time Out: 3

☐ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
☑ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	☐ Enable	1.11		

Set IP

IP Setting

IP Mode: Static IP Address

IP Address: 192 . 168 . 0 . 50

Sub Mask: 255 . 255 . 255 . 0

Gateway: 0 . 0 . 0 . 0

DNS: . . .

Get gateway done

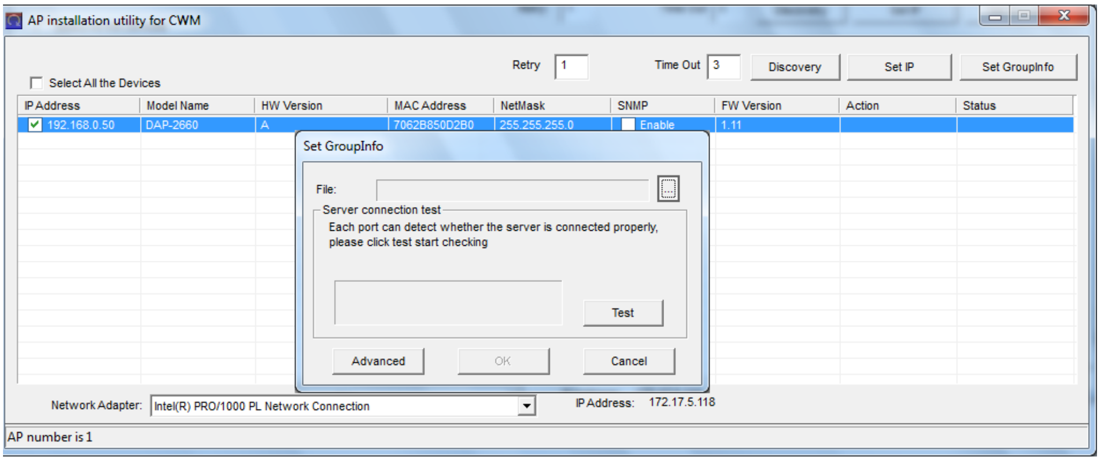
Network Adapter: Intel(R) PRO/1000 PL Network Connectio

AP number is 1

Figure 5-8 AP Installation Utility for CWM (Set IP)

After clicking the **OK** button to set the IP address settings, the access point will be configured and some time will be given for the access point to restart after the new IP address settings was applied. The **Status** parameter will display the progress of the IP address configuration and access point reboot.

This utility also allows us to upload the network data file directly to the access point to configure the group information that this access point will use to identify in which network it belongs. Click the **Set GroupInfo** button to upload the network data file. After click the **Set GroupInfo** button, we can click on the "**...**" button to navigate to the saved network data file on the computer and then upload it.



AP installation utility for CWM

Retry: 1 Time Out: 3

☐ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
☑ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	☐ Enable	1.11		

Set GroupInfo

File:

Server connection test

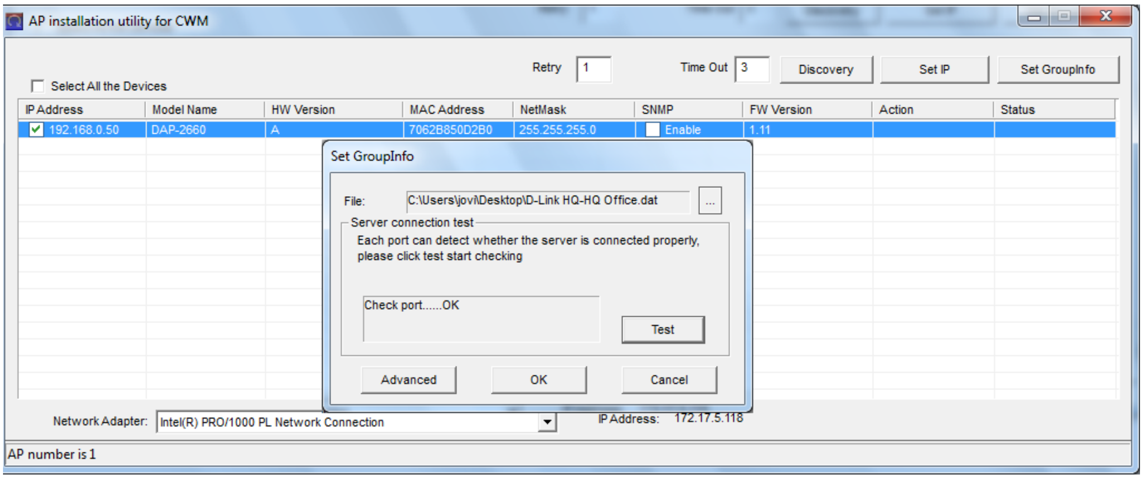
Each port can detect whether the server is connected properly, please click test start checking

Network Adapter: Intel(R) PRO/1000 PL Network Connection IP Address: 172.17.5.118

AP number is 1

Figure 5-9 AP Installation Utility for CWM (Set Groupinfo)

Click the **Test** button to test if the data file is in fact a valid network data file. After clicking the **Test** button to successfully test if the network data file is valid, the following message will be displayed. Click the **OK** button to initiate the upload.



AP installation utility for CWM

Retry: 1 Time Out: 3

☐ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
☑ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	☐ Enable	1.11		

Set GroupInfo

File: C:\Users\jovi\Desktop\D-Link HQ-HQ Office.dat

Server connection test

Each port can detect whether the server is connected properly, please click test start checking

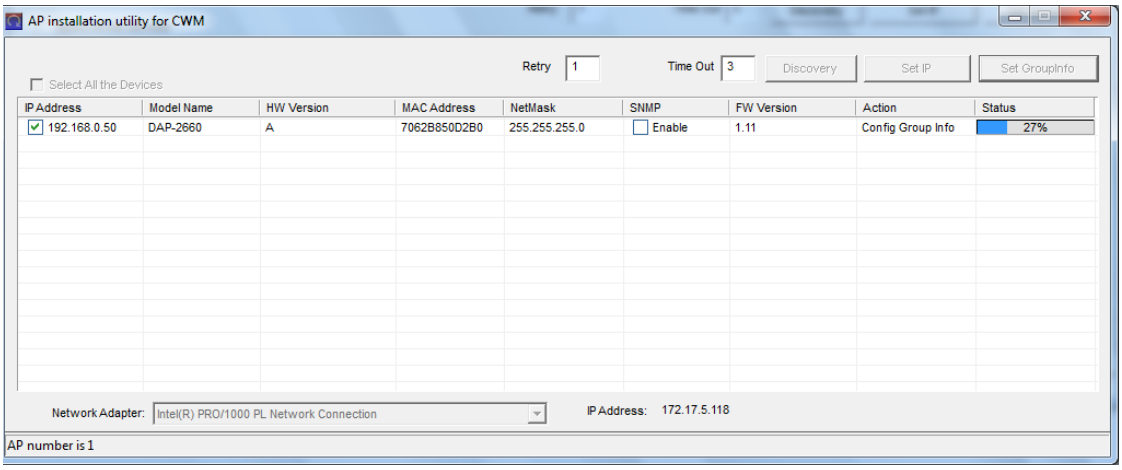
Check port......OK

Network Adapter: Intel(R) PRO/1000 PL Network Connection IP Address: 172.17.5.118

AP number is 1

Figure 5-10 AP Installation Utility for CWM (Test, OK)

After clicking the **OK** button, the network data file will be uploaded, the access point will be configured based on the settings within the data file, and will then reboot. The **Status** parameter will display the progress of the configuration.



Retry 1 Time Out 3

□ Select All the Devices

IP Address	Model Name	HW Version	MAC Address	NetMask	SNMP	FW Version	Action	Status
☑ 192.168.0.50	DAP-2660	A	7062B850D2B0	255.255.255.0	□ Enable	1.11	Config Group Info	27%

Network Adapter: Intel(R) PRO/1000 PL Network Connection

IP Address: 172.17.5.118

AP number is 1

Figure 5-11 AP Installation Utility for CWM (Uploading, Reboot)