



# Application Note 56

---

**Hotspot feature for Wi-Fi clients with  
RADIUS User Authentication on Digi  
TransPort.**

Digi Support  
November 2015

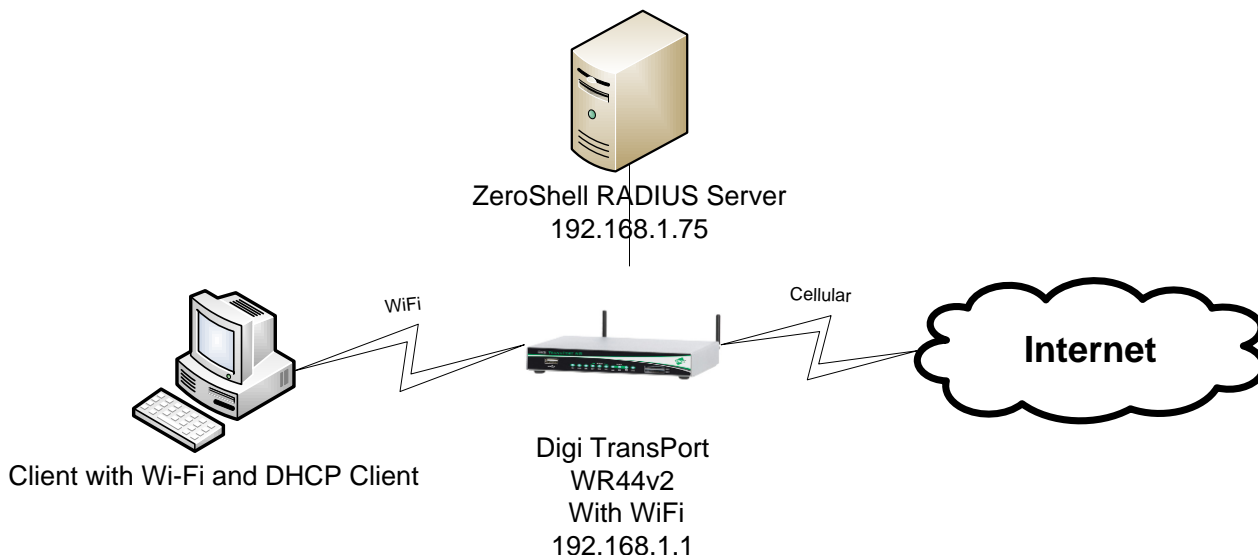
# Contents

1	Introduction.....	4
1.1	Outline.....	4
1.2	Assumptions.....	4
1.3	Corrections.....	4
2	Version.....	5
3	Configuration.....	5
3.1	Mobile Interface Configuration.....	5
3.2	Ethernet Interface Configuration.....	6
3.2.1	ETH 0 Configuration.....	6
3.2.2	ETH 12 Logical Interface Configuration.....	7
3.3	DHCP “Wi-Fi Only” Configuration for ETH 12.....	8
3.4	Wi-Fi Interface Configuration.....	9
3.4.1	Wi-Fi Global Settings Configuration.....	9
3.4.2	Wi-Fi Node 0 Configuration.....	10
3.4.3	RADIUS Client Configuration.....	11
3.4.4	Wi-Fi Hotspot Configuration.....	12
4	Radius server configuration.....	14
4.1	Configuration overview.....	14
4.2	Create ZeroShell live CD.....	14
4.3	Configure ZeroShell network settings.....	14
4.4	Configure profile and save settings.....	15
4.5	Generate CA certificate and private key.....	16
4.6	Create remote user account.....	17
4.7	Export remote user certificate.....	18
4.8	Export Trusted CA certificate.....	19
4.9	Create authorized client.....	19
5	Connect to the Wi-Fi Hotspot.....	21
6	Testing.....	23
6.1	Checking Wi-Fi connection status.....	23
6.1.1	Web GUI.....	23
6.1.2	Command Line (CLI).....	24
	The command wificonn will display all the Wi-Fi clients connected and their status.....	24
	The command dhcp 12 status will display the DHCP Server status of Interface ETH 12.....	24

6.1.3	Checking RADIUS Authentication logs.....	24
7	Configuration files .....	25
8	Customization .....	28
8.1	Configure Splashpage for WI-FI Hotspot.....	28
8.2	Change the image file .....	31
8.3	Load new splashpage and images onto the TransPort .....	31
9	Splashpage example file .....	33

# 1 INTRODUCTION

## 1.1 Outline



This document describes how to configure a Digi TransPort as a Wi-Fi Hotspot Access Point and Radius authentication to provide Wi-Fi clients with Internet access through Cellular.

## 1.2 Assumptions

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product and of the requirements for their specific application. It also assumes a basic ability to access and navigate a Digi TransPort router.

This application note applies only to:

**Model:** DIGI TransPort WR41/44 with the Wi-Fi option.

**Firmware versions:** 5169 and later

**Configuration:** This document assumes that the devices are set to their factory default configurations. Most configuration commands are shown only if they differ from the factory default.

**Please note:** This application note has been specifically rewritten for firmware release 5169 and later and will not work on earlier versions of firmware. Please contact [tech.support@digicom.com](mailto:tech.support@digicom.com) if you require assistance in upgrading the firmware of the TransPort router.

## 1.3 Corrections

Requests for corrections or amendments to this application note are welcome and should be addressed to: [tech.support@digicom.com](mailto:tech.support@digicom.com)

Requests for new application notes can be sent to the same address.

## 2 VERSION

Version Number	Status
1.0	Published

## 3 CONFIGURATION

### 3.1 Mobile Interface Configuration

Configuration – Network > Interfaces > Mobile > Mobile Settings

Configure the Mobile settings for the SIM card to provide cellular connection to the Digi TransPort and allow Wi-Fi clients to have internet access through it.

**Configuration - Network > Interfaces > Mobile**

**Mobile**

Select a SIM to configure from the list below

Settings on this page apply to the selected SIM

SIM: 1 (PPP) (Optional)

IMSI: 2080140031004134

**Mobile Settings**

Select the service plan and connection settings used in connecting to the mobile network.

**Mobile Service Provider Settings**

Use custom APN instead of built-in APN

Custom APN: internet

SIM PIN: ●●●●●● (Optional)

Confirm SIM PIN:

Username: user (Optional)

Password: ●●●●●● (Optional)

Confirm Password:

**Mobile Connection Settings**

Re-establish connection when no data is received for a period of time

**Mobile Network Settings**

Enable NAT on this interface

IP address  IP address and Port

Parameter	Setting	Description
SIM	1(PPP1)	SIM card slot where the SIM card is inserted
APN	Internet	APN associated with the SIM card
SIM PIN	****	SIM PIN if there is one configured, else, leave blank.
Confirm SIM PIN	****	Confirm the SIM PIN if there is one configured, else, leave blank.
Username	User	Username for the configured APN. If not required, leave blank.
Password	****	Password for configured APN username. If not required, leave blank.
Confirm Password	****	Confirm password for configured APN username. If not required, leave blank.
Enable NAT on this Interface	Checked	Enable NAT on the PPP1 interface (IP Address is sufficient for most configuration)

Click **Apply** and **Save** to save the settings.

## 3.2 Ethernet Interface Configuration

### 3.2.1 ETH 0 Configuration

Configuration – Network > Interfaces > Ethernet > ETH 0

The screenshot shows the configuration window for the Ethernet interface ETH 0. It includes a description field, two radio button options for IP addressing (DHCP and manual settings), and two input fields for the IP address (192.168.1.1) and subnet mask (255.255.255.0). The IP address and mask fields are highlighted with a red border.

Parameter	Setting	Description
IP Address	192.168.1.1	IP Address of the Router's ETH 0 interface
Mask	255.255.255.0	Subnet Mask of the Router's ETH 0 interface

### 3.2.2 ETH 12 Logical Interface Configuration

Logical Interface Ethernet 12 will be used for Wi-Fi clients.

Configuration – Network > Interfaces > Ethernet > ETH 12

▼ ETH 12

Description:

Get an IP address automatically using DHCP

Use the following settings

IP Address:

Mask:

Parameter	Setting	Description
IP Address	10.10.10.1	IP Address of the Router's ETH 12 logical interface
Mask	255.255.255.0	Subnet Mask of the Router's ETH 12 logical interface

Configuration – Network > Interfaces > Ethernet > ETH 12 > Advanced

Configure the port to « Port Isolate mode »

▼ Advanced

This device is currently in Hub mode

Ethernet Hub group:

Parameter	Setting	Description
Switch to Port Isolate mode	Click	In Port Isolate mode the router will only respond to its Ethernet IP address on physical port. This port will be bridged to the Wi-Fi instance.

Click **Apply** and **Save** to save the settings.

**You must reboot for this change to take effect**

### 3.3 DHCP “Wi-Fi Only” Configuration for ETH 12

In this example, the Digi TransPort router will have a dedicated DHCP server for Wi-Fi clients only.

Configuration – Network > DHCP Server > Logical Ethernet Interfaces > DHCP Server for Ethernet 12

**▼ DHCP Server for Ethernet 12**

Enable DHCP Server

IP Addresses: 10.10.10.100 to 10.10.10.200

Mask: 255.255.255.0

Gateway: 10.10.10.1

DNS Server: 10.10.10.1

Secondary DNS Server: 8.8.8.8

Domain Name: wifi.digi.com

Lease Duration: 14 days 0 hrs 0 mins

Wait for 0 milliseconds before sending DHCP offer reply

Only send offers to Wi-Fi clients

**DHCP Relay**

Forward DHCP requests to:

▶ **Advanced**

▶ **Advanced DHCP Options**

Apply



Parameter	Setting	Description
Enable DHCP Server	Checked	Enable DHCP Server for this interface
IP Addresses	10.10.10.100 – 10.10.10.200	Start and End of DHCP Range
Mask	255.255.255.0	DHCP Server Subnet mask for this interface. This must match the settings of Ethernet 12
Gateway	10.10.10.1	Gateway address. This must match ETH 12 address
DNS Server	10.10.10.1	Primary DNS Server, by default the TransPort will act as a DNS Server. This must match ETH 12 Address.
Secondary DNS Server	8.8.8.8	Set a Secondary DNS Server if required (in this example, Google's public DNS Server)
Domain Name	*	Set the domain name to be used by the Wi-Fi clients.
Only send offers to Wi-Fi clients	Checked	Select this option to only send DHCP offers on this interface to Wi-Fi clients.

## 3.4 Wi-Fi Interface Configuration

### 3.4.1 Wi-Fi Global Settings Configuration

Configuration – Network > Interfaces > Wi-Fi > Global Wi-Fi Settings

Global Wi-Fi Settings

Country: France

Remote management access: Disable management

Network Mode: B/G/

Channel: Aut

Antenna: Auto

▶ Advanced

▶ Wi-Fi Hotspot

▶ Wi-Fi Filtering

Apply

Parameter	Setting	Description
Country	<Chose>	Select the Country where the device is used
Remote management access	Disable management	Do not allow Wi-Fi clients to log into the device and manage it
Network Mode	B/G/N	Chose which network mode to use
Channel	Auto	Let the router chose the best channel to use
Antenna	Auto	Use both Antennas for Wi-Fi

### 3.4.2 Wi-Fi Node o Configuration

Configuration – Network > Interfaces > Wi-Fi > Wi-Fi Node o

**Wi-Fi Node 0 - TransPort Hotspot**

Enable this Wi-Fi interface

Description:

SSID:

Mode:

In order to send data to and from this Wi-Fi interface, it must be bridged with at least one Ethernet interface. This Wi-Fi interface is a member of Bridge instance  and therefore bridged to the following interfaces

Interface	
<input type="text" value="Ethernet"/>	<input type="text" value="12"/> <input type="button" value="Delete"/>
<input type="text" value="Ethernet"/>	<input type="button" value="Add"/>

Hide SSID

Enable station isolation

Click [here](#) to assign a timeband to this interface

**Wi-Fi Security**

Use the following security on this Wi-Fi interface:

None  WEP  WPA-PSK  WPA2-PSK  WPA-802.1X  WPA2-802.1X

**Network Scanning**

Parameter	Setting	Description
Enable this Wi-Fi interface	Checked	Enable Wi-Fi Node o interface
Description	TransPort Hotspot	Enter a description for this interface
SSID	Hotspot	SSID used for the hotspot and for clients to connect
Mode	Access Point	Wi-Fi mode for this interface
This Wi-Fi interface is a member of Bridge instance	1	Select the Bridge Instance 1 which contains Ethernet 12
Interface	Ethernet 12	Bridge this Wi-Fi interface with Ethernet 12
Enable station isolation	Checked	Station isolation will prevent wi-fi clients connected on the hotspot to communicate and be isolated.

Click **Apply** and **Save** to save the settings.

### 3.4.3 RADIUS Client Configuration

Configuration – Security > RADIUS > RADIUS Client5

**▼ RADIUS Client5**

RADIUS can be used to authenticate remote command, SSH, FTP and Web sessions. You can configure two servers. The secondary server is used if there is no response from the primary server.

Local authentication can be used if there is no response from the configured servers.

RADIUS accounting can be used to log authentication attempts.

**Authorization**

**Primary Authorization Server**

Hostname:

NAS ID:

Password:

Confirm Password:

Parameter	Setting	Description
Hostname	192.168.1.75	Enter the IP Address used for the ZeroShell RADIUS server (in this example 192.168.1.75)
NAS ID	ZSHELL	Enter the NAS ID configured into the Radius server (in this example "ZSHELL" is used)
Password	digitest	Enter the shared key that is used to authenticate requests from this NAS to the Radius server (in this example "digitest" is used)
Confirm Password	digitest	Confirm the shared key that is used to authenticate requests from this NAS to the Radius server (in this example "digitest" is used)

Click **Apply** and **Save** to save the settings.

### 3.4.4 Wi-Fi Hotspot Configuration

Configuration – Network > Interfaces > Wi-Fi > Global Wi-Fi Settings > Wi-Fi Hotspot

**Wi-Fi Hotspot**

Enable Wi-Fi Hotspot on

Wi-Fi Node 0  Disabled  HTTP Redirect Mode  **DNS Redirect Mode**  
 Wi-Fi Node 1  Disabled  HTTP Redirect Mode  DNS Redirect Mode  
 Wi-Fi Node 2  Disabled  HTTP Redirect Mode  DNS Redirect Mode  
 Wi-Fi Node 3  Disabled  HTTP Redirect Mode  DNS Redirect Mode

Splashscreen filename:

Each client can connect for:  hrs  mins

Require Wi-Fi Client Authentication

Use RADIUS instance:

You can configure up to 4 hotspot exceptions

Hostname
www.digi.com <span style="float: right;">Delete</span>
<input type="text"/> <span style="float: right;">Add</span>

**Wi-Fi Filtering**

Parameter	Setting	Description
Enable Wi-Fi Hotspot on Wi-Fi Node o	DNS Redirect Mode	<b>DNS Redirect Mode</b> will result in the Transport intercepting any DNS queries and return its own address instead of the real address. <b>HTTP Redirect Mode</b> will authorise DNS queries to external server but web requests will be redirected to the router hotspot page prior to allow general network access
Splashscreen filename	hs_login.asp	User Authentication Splashscreen web page file name to be used when clients connects the first time.
Each client can connect for	1 hrs	Time to allow clients to connect to before forcing a reconnection
Require Wi-Fi Client Authentication	Checked	Turn ON Wi-Fi client authentication to the ZeroShell Radius server
Use RADIUS instance	5	Use RADIUS instance 5 configuration
Hostname	<a href="http://www.digi.com">www.digi.com</a>	Optional : Allow domains exceptions (up to 4) that you wish to provide unrestricted access to (Clients connected and visiting this domain will not be required to accept the terms or authenticate on the hotspot splash screen page)

Click **Apply** and **Save** to save the settings.

## 4 RADIUS SERVER CONFIGURATION

### 4.1 Configuration overview

In this Application note, the ZeroShell Linux distribution (can be booted from live CD, USB or VMWare) will be used to configure a Radius server for WPA Authentication of the Wi-Fi Hotspot clients.

The latest version of ZeroShell can be downloaded from: <http://www.zeroshell.org/download/>

Steps 4.2 to 4.4 will go through downloading, booting and configuring ZeroShell

Steps 4.5 to 4.8 will go through Radius configuration and generally apply to any Radius server.

### 4.2 Create ZeroShell live CD

Download the latest version of ZeroShell from the web site above. There are number of versions available. The "ISO image for CD" version 3.1.0 booted under VMWare was used for this Application Note.

It is also possible to create a CD containing this image using the appropriate CD-burning software such as <http://cdburnerxp.se/en/home>.

When the CD has been created, choose an appropriate computer to act as the Radius server (not the one used to test the Wi-Fi hotspot) and boot it from the CD (it may be necessary to change the computer's boot sequence to allow booting from the CD). ZeroShell does not require an especially fast computer, an old laptop or desktop machine can be used for this test.

### 4.3 Configure ZeroShell network settings

Once ZeroShell server has booted, a command line interface prompt is used to configure the IP address, mask, gateway and setting the admin password.

- Type option: **<I> IP Manager**
- Select: **<M> Modify IP address**
- Press Enter to configure the default Ethernet address: **Interface [ETH0]:**
- Press Enter once more: **IP to modify [1]:**
- Type in the IP address for this interface. For this example 192.168.1.75 was used for the server address: **IP [192.168.1.1]: 192.168.1.75**
- Type in the subnet mask to be used for this connection. For this example the default 24-bit mask is correct, so simply pressing Enter leaves the mask as the default value: **Netmask [255.255.255.0]:**
- IP Status should be showing as "up": **IP status [up]:**
- Press Enter to return to the previous menu

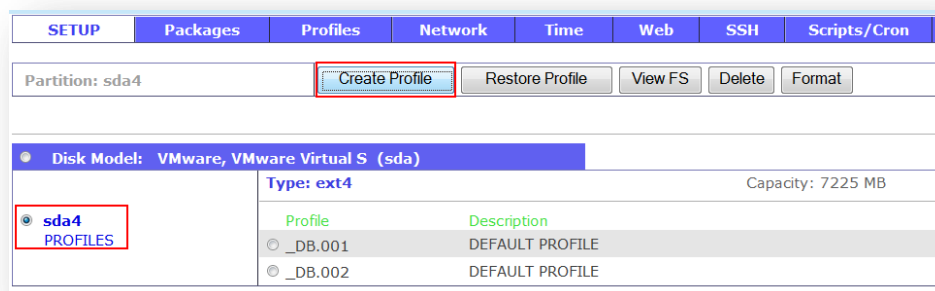
- Type option: **<G> Set Default Gateway**
- Enter the default gateway address For this example 192.168.1.1 was used: **Default Gateway: 192.168.1.1**
- Type option: **<Q> Quit** (to previous menu)
- Type option: **<P> Change admin password**
- If prompted for the current admin password, type in the existing password - by default this may be 'ZeroShell'. However the default password may simply be blank, therefore it may be possible to simply press Enter when prompted for the current admin password.
- Enter the new password: **New admin password: <NEW\_PASSWORD>**
- Confirm the new password: **Confirm password: <NEW\_PASSWORD>**

It should be now possible to open a web browser and navigate to <https://192.168.1.75> in order to configure the ZeroShell server via its web interface. Log in using the username **admin** and the admin password that was configured via the command line interface previously.

## 4.4 Configure profile and save settings

This step ensures that the ZeroShell server's settings can be saved to a USB flash drive or hard drive, since the live CD is read-only. ZeroShell supports the saving of profiles to disks with ext2, ext3, ReiserFS or FAT32 filesystems. It includes an in-built formatting utility, so for example it is possible to format a USB flash drive from within the ZeroShell interface. For this example the VMWare local hard disk (ext4-formatted) was used.

- Select **Setup** from the **System** section of the left hand menu
- Select **Profiles**
- Select a partition to save the profile to – it may take a short while for the drive scan to complete:



A pop-up window will then prompt for the following parameters:

- Enter a **Description**
- Enter the **Hostname (FQDN)** of the server
- Enter a **Kerberos 5 Realm**
- Enter the **LDAP Base**
- Enter and confirm the **Admin Password** in the next two fields
- Select the correct **Ethernet Interface** (or accept the default if this is correct)
- Enter the **IP Address/Netmask** and **Default Gateway**
- Click **Create**

**VMware, VMware Virtual S (sda)** Create Close

New Profile on partition sda4

---

Description: Hotspot WiFi

Hostname (FQDN): testwifi.digi.com

Kerberos 5 Realm: DIGI.COM

LDAP Base: dc=digi,dc=com

Admin password: ●●●●

Confirm password: ●●●●

**NETWORK CONFIG**

Ethernet Interface: ETH00 - Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE] (re ▼)

IP Address / Netmask: 192.168.1.75 / 255.255.255.0

Default Gateway: 192.168.1.1

Saved profiles can be activated, deactivated, deleted or backed up from the following page:

SETUP Packages Profiles Network Time Web SSH Scripts/Cron

Profile: \_DB.003 (sda4) Activate Deactivate Info Delete Backup Backup without Logs Copy Create

---

● Disk Model: VMware, VMware Virtual S (sda) Type: ext4 Capacity: 7225 MB

Profile	Description
<input type="radio"/> _DB.001	DEFAULT PROFILE
<input type="radio"/> _DB.002	DEFAULT PROFILE
<input checked="" type="radio"/> <u>_DB.003</u>	<u>Hotspot WiFi</u>

## 4.5 Generate CA certificate and private key

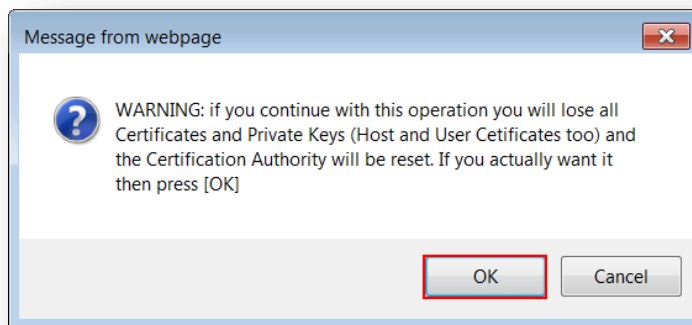
**Please note:** any desired changes to the default parameters for the CA (please see lower section in Figure 9 below) need to be applied *before* following the steps below.

- Select **X.509 CA** from the **Security** section on the left hand menu
- Select **Setup** from the top menu
- Enter the **Common Name** you wish to use for the CA certificate
- Enter the **Key Size**
- Enter the **Country Name**
- Enter the **State or Province**
- Enter the **Locality**
- Enter the **Organization**
- Enter the **Operational Unit**
- Enter the **Email Address**
- Click **Generate** on the right side of the web interface



X.509 CA	List	Manage	CRL	Imported	Trusted CAs	Setup
<b>CA Certificate and Private Key</b>						
Common Name						Hotspot
Key Size						2048 bits
Validity (Days)						365
Country Name						DE
State or Province						None
Locality						Munich
Organization						digi.com
Organizational Unit						TechSupport
E-Mail Address						tech.support@digi.com
<b>CA Default Parameters</b>						Apply
Key Size						2048 bits
Certificate Validity (days)						730
Export user/host certificates on the authentication page						No

A prompt will be seen warning that existing certificates will be deleted. Click **OK** to proceed



## 4.6 Create remote user account

It is necessary to configure one or more remote user accounts, to enable Wi-Fi clients to authenticate with the Radius server. For this example only one remote user is configured:

- Select **Users** under the **Users** section of the left hand menu
- Click **Add**
- Enter a **Username** for the remote user
- Enter a **Firstname**
- Enter a **Lastname**
- Enter a **Password** then **Confirm** by entering it again - in this example **testuserpass** was used

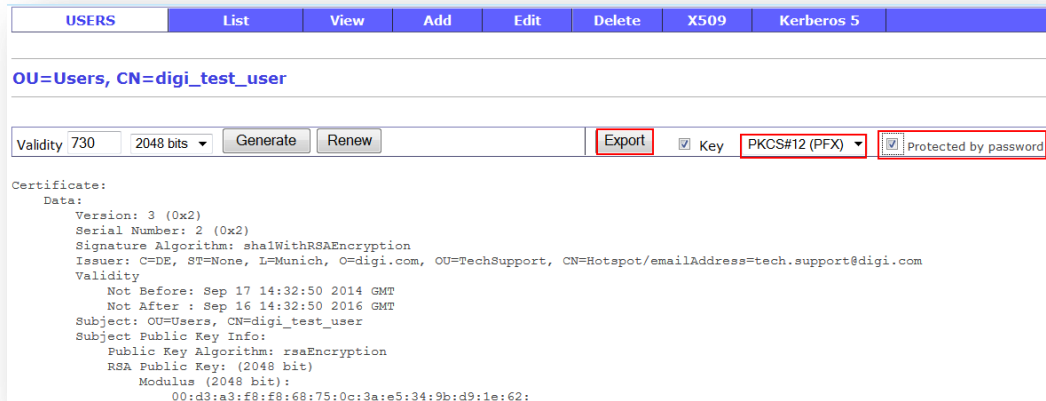
- Other fields such as **Description** and **E-Mail** are optional
- Click **Submit** on the right side of the web interface

USERS	List	View	Add	Edit	Delete	X509	Kerberos 5
<b>(New User)</b>							
<b>Account Information</b>							
Username <input type="text" value="digi_test_user"/>		UID <input type="text"/>					
Home Directory <input type="text"/>						Default Shell	
<b>User Information</b>							
Firstname <input type="text" value="firstname"/>		Lastname <input type="text" value="lastname"/>					
Description <input type="text"/>				E-Mail <input type="text"/>			
<b>RADIUS Accounting</b>							
Expiration (mm/dd/yyyy) <input type="text"/>		Accounting Class <input type="text" value="DEFAULT"/>					
Credit: 0.00 € <input type="text"/>		Limits <input type="text" value="- MB   - h   - Mb/s"/>		Costs (postpaid) <input type="text" value="0.00€/MB   0.00€/h"/>			
						<b>User Password</b>	
						Password <input type="password" value="••••••"/>	
						Confirm <input type="password" value="••••••"/>	

The ZeroShell server will now provide the option to export the user certificate – please see section 4.7 below.

## Export remote user certificate

This example uses a Windows laptop as the remote access client, so it is necessary to export the user certificate using the “.pfx” format so that it can be imported in the Windows Certificate Management. The user certificate includes the Radius server’s private key in addition to the certificate itself. The file should be protected with a password, so before clicking **Export** please ensure that the **Protected by Password** option is ticked as shown:



This ensures that the “.pfx” file is protected by the password that was configured in the above step to create the user account. When the file is imported in Windows, the password will need to be entered to allow the certificate to be installed.

## 4.8 Export Trusted CA certificate

- Select **RADIUS**
- Select **Trusted CAs**
- In the Trusted CAs list, click on the **Hotspot** entry
- Click the **Export** button
- Save the file to a location on the computer



## Create authorized client

It is necessary to add the TransPort router as an authorized client in order to allow it to communicate with the ZeroShell server, and therefore to relay authentication traffic from and to the Wi-Fi client. Authentication between the TransPort router and the ZeroShell server is accomplished via a shared secret:

- Select **Radius** under the **Users** section of the left hand menu
- Select **Authorized Clients**
- Enter the **Client Name** (NAS ID) – in this example **ZSHELL** was used
- Enter the **IP or Subnet** of the TransPort router – in this example **192.168.1.1/32** was used
- Enter the **Shared Secret** – this must be the same as the “Radius server password” that was configured in the TransPort router - in this example **digitest** was used
- Click **+** to add this client

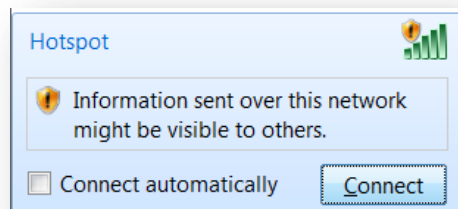
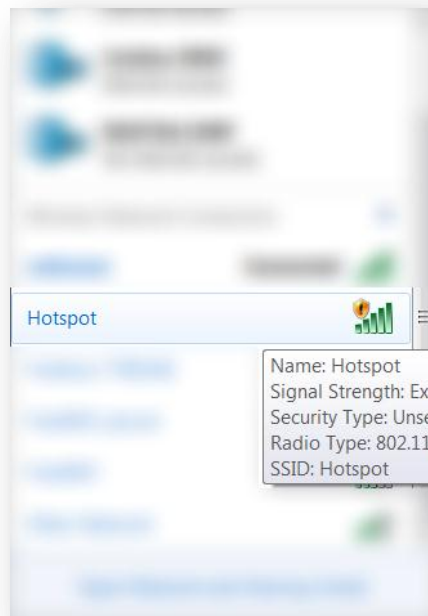
Client Name	IP or Subnet	Shared Secret
ZSHELL	192.168.1.1 / 32	digitest

## 5 CONNECT TO THE WI-FI HOTSPOT

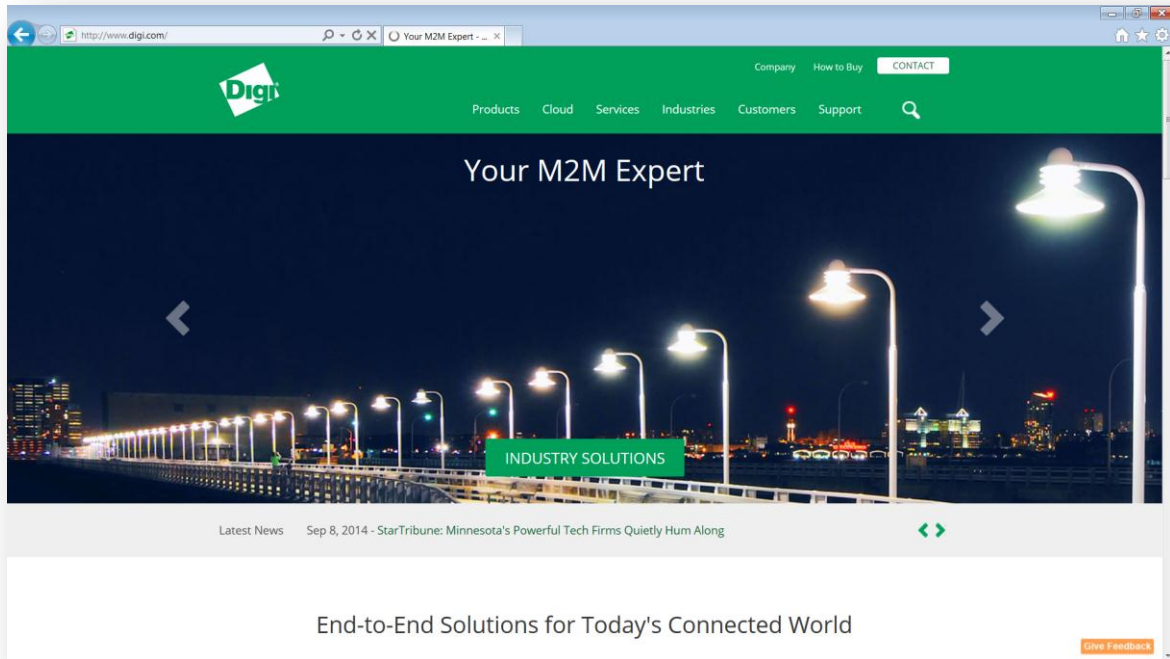
Under Windows 7/8, Right Click on the Wi-Fi icon in the task bar



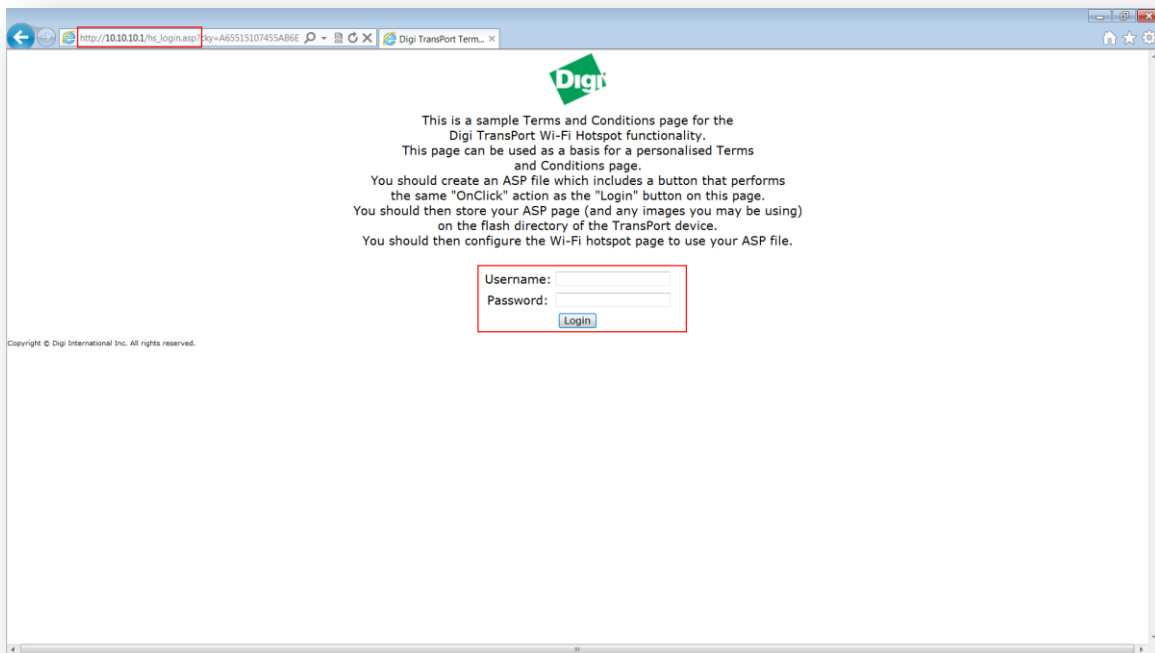
This should bring the Wireless network Connection menu. The "Hotspot" SSID should appear with "No Security". Select it and click **Connect** to connect to the Hotspot.



Opening a web browser to one of the Hotspot's exceptions will display the page directly (like <http://www.digi.com> in our example)



However, opening a web browser to any other domain will prompt the user to login (using the previously created **digi\_test\_user** on the RADIUS server) and accept terms and conditions from the standard `hs_login.asp` page. This page can be customized or replaced by another page of your choosing and selected like shown in section [3.4.3](#)



Upon clicking on **Login**, the web page will redirect to the right site.

## 6 TESTING

### 6.1 Checking Wi-Fi connection status

#### 6.1.1 Web GUI

You can check the number of connected clients and their status on the Wi-Fi management page.

#### Management – Network Status > Interfaces > Wi-Fi

Module Detected: Yes (168C:002A)  
Admin Status: Up  
Operational Status: Up  
Channel Mode: B/G/N  
Channel: 1  
MAC Address: 04:f0:21:0a:59:03

Bytes Received: 1080233      Bytes Sent: 1797928  
Packets Received: 12066      Packets Sent: 9286  
Receive Errors: 229      Transmit Errors: 31  
Received Packets Dropped: 0

Number of Connected Wi-Fi Clients: 1

Node	Wi-Fi Node	RSSI	Flags	Power Save	Mode	Neg. Rates (Mbps)	TX Rate (Mbps)	RX Rate (Mbps)	Capability Info
8c:70:8c:70:8c:70	0	42	ERP,	Awake	N	6.5, 13.0, 19.5, 26.0, 39.0, 52.0, 58.5, 65.0, 13.0, 26.0, 39.0, 52.0, 78.0, 104.0, 117.0, 130.0	130.0	130.0	ESS, Short Preamble, Short Slottime, <a href="#">Disconnect</a>

[Disconnect All Clients](#)

Number of Access Point Connections: 0

[Refresh](#)

You can also check the DHCP status for clients under the DHCP Status page

IP address	Hostname	Lease time left (mins)
192.168.1.100		19288
192.168.1.101		19452
10.10.10.100	DOR	20149

[Clear DHCP Entries](#)

## 6.1.2 Command Line (CLI)

The command **wificonn** will display all the Wi-Fi clients connected and their status

```
Number of connected clients: 1
Number of client mode connections: 0

 1 Node 8c:70:8c:70:8c:70
   Wi-Fi node : 0
   RSSI      : 42
   Flags     : ERP
   Power Save : Awake
   Mode      : N
   Neg. Rates : 6.5 13.0 19.5 26.0 39.0 52.0 58.5 65.0 13.0 26.0 39.0 52.0 78.0
104.0 117.0 130.0 Mbps
   TX Rate   : 117.0 Mbps
   RX Rate   : 130.0 Mbps
   Cap. Info : ESS Short_Preamble Short_Slottime
   HT Cap.   : GREENFIELD SHORTGI20 RXSTBC(1) AMSDU(7935)
   Channel   : 1

OK
```

The command **dhcp 12 status** will display the DHCP Server status of Interface ETH 12

```
Entry: IP [192.168.1.100], hostname [], MAC [00:10:49:31:27:a8], expiry 19282 (mins)
Entry: IP [192.168.1.101], hostname [], MAC [00:40:9d:4a:1d:4c], expiry 19446 (mins)
Entry: IP [10.10.10.100], hostname [DOR], MAC [8c:70:8c:70:8c:70], expiry 20143 (mins)
OK
```

### Checking RADIUS Authentication logs

Under: **System**, click on **Logs**.

You should be able to see this entry after a user has entered their login and password on the Splashpage :

```
01:01:18 Login OK: [digi_test_user] (from client ZSHELL port 0 via TLS tunnel)
01:01:18 Login OK: [digi_test_user] (from client ZSHELL port 0)
```



## 7 CONFIGURATION FILES

### Digi TransPort WR44v2

```
wifi 0 country "France"
wifi 0 chanmode "bgn"
wifi 0 hotspot_fname "hs_login.asp"
wifi 0 hotspot_lifetime 60
wifi 0 hotspot_auth ON
wifi 0 hotspot_radiuscfg 5
wifi 0 nocfg 1
wifinode 0 descr "TransPort Hotspot"
wifinode 0 ssid "Hotspot"
wifinode 0 hotspot 2
wifinode 0 isolation ON
wifinode 0 bridge_inst 1
eth 0 IPAddr "192.168.1.44"
eth 0 DNSserver "192.168.1.1"
eth 0 gateway "192.168.1.1"
eth 0 do_nat 2
eth 0 bridge ON
eth 12 IPAddr "10.10.10.1"
eth 12 do_nat 2
eth 12 bridge ON
eth 12 bridge_inst 1
eth 12 ipanon ON
eth 12 physadd -1
addp 0 enable ON
lapb 0 ans OFF
lapb 0 tinact 120
lapb 1 tinact 120
lapb 3 dtemode 0
lapb 4 dtemode 0
lapb 5 dtemode 0
lapb 6 dtemode 0
gps 0 asy_add 1
gps 0 gpson ON
ip 0 cidr ON
def_route 0 ll_
hshosts 0 host "www.digi.com"
dhcp 0 respdelms 500
dhcp 0 mask "255.255.255.0"
dhcp 0 gateway "192.168.1.1"
dhcp 0 DNS "
dhcp 12 IPmin "10.10.10.100"
dhcp 12 IPrange 101
dhcp 12 lease 60
dhcp 12 wifionly ON
dhcp 12 mask "255.255.255.0"
dhcp 12 gateway "10.10.10.1"
dhcp 12 DNS "10.10.10.1"
sntp 0 server "time.etherios.com"
ppp 0 timeout 300
ppp 1 name "W-WAN"
ppp 1 phonenumber "*98*3#"
ppp 1 username "username"
ppp 1 epassword "KD51SVJDVVg="
ppp 1 IPAddr "0.0.0.0"
ppp 1 timeout 0
```

```
ppp 1 use_modem 1
ppp 1 cdma_backoff ON
ppp 1 aodion 1
ppp 1 autoassert 1
ppp 1 pwr_dly 40
ppp 1 r_chap OFF
ppp 3 name "DSL"
ppp 3 l1iface "AAL"
ppp 3 username "Enter ADSL Username"
ppp 3 r_addr OFF
ppp 3 IPaddr "0.0.0.0"
ppp 3 l_addr ON
ppp 3 timeout 0
ppp 3 do_nat 2
ppp 3 aodion 1
ppp 3 autoassert 1
ppp 3 immoos ON
ppp 3 echo 10
ppp 3 echodropcnt 5
ppp 3 l_pap OFF
ppp 3 l_chap OFF
ppp 3 defpak 16
ppp 4 defpak 16
web 0 prelogin_info ON
modemcc 0 info_asy_add 7
modemcc 0 apn "none"
modemcc 0 link_retries 30
modemcc 0 stat_retries 30
modemcc 0 sms_interval 1
modemcc 0 sms_access 1
modemcc 0 sms_concat 0
modemcc 0 apn_2 "none"
modemcc 0 link_retries_2 30
modemcc 0 stat_retries_2 30
modemcc 0 sms_interval_2 1
modemcc 0 sms_access_2 1
ana 0 anon ON
ana 0 l2on OFF
ana 0 xoton OFF
ana 0 lapdon 0
ana 0 lapbon 0
ana 0 logsize 45
cmd 0 unitid "ss%s>"
cmd 0 cmdnua "99"
cmd 0 hostname "digi.router"
cmd 0 asyled_mode 2
cmd 0 tremto 1200
cmd 0 rcihttp ON
cmd 1 autocmd "ats31=7"
cmd 1 gpson ON
cmd 4 cmd_processor OFF
user 0 access 0
user 1 name "username"
user 1 epassword "KD51SVJDVVg="
user 1 access 0
user 2 access 0
user 3 access 0
user 4 access 0
user 5 access 0
user 6 access 0
user 7 access 0
user 8 access 0
```

```
user 9 access 0
local 0 transaccess 2
sslsvr 0 certfile "cert01.pem"
sslsvr 0 keyfile "priv
radcli 5 nasid "ZSHELL"
radcli 5 server "192.168.1.75"
radcli 5 epassword "PDZxU1FJVEg="
ssh 0 hostkey1 "privSSH.pem"
ssh 0 nb_listen 5
ssh 0 v1 OFF
cloud 0 ssl ON
```

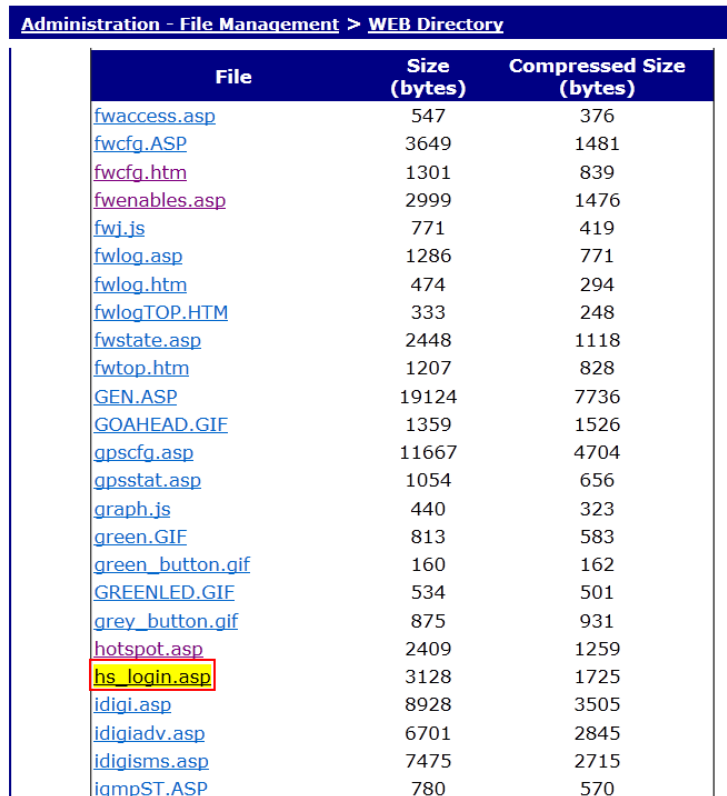
## 8 CUSTOMIZATION

This section describes how to create your own "Splash-screen" or "disclaimer" page on Digi TransPort Wi-Fi routers, and how to add your own graphics to the page. This "Splash-screen" page is shown when Wi-Fi users first access the Internet or external websites. A timer can be set so that users must "re-authenticate" via this page when the timer expires.

Refer to the Digi TransPort User Guide and Application Notes posted on [www.digi.com/support](http://www.digi.com/support) for full details.

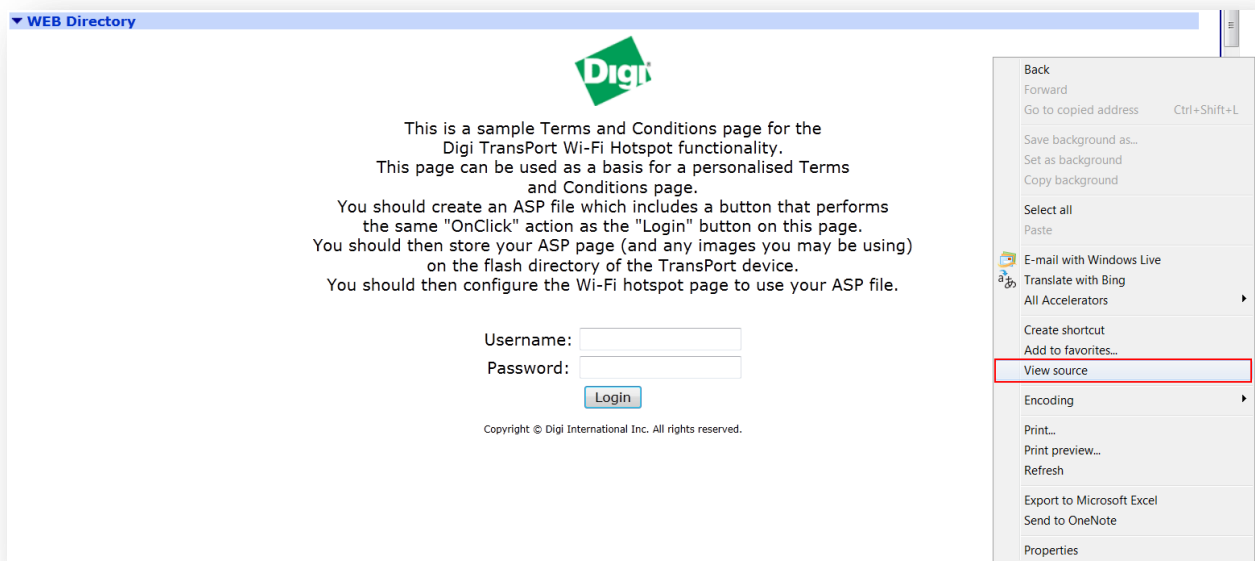
### 8.1 Configure Splashpage for WI-FI Hotspot

Download the sample **hs\_login.asp** file. Go to **Administration-File Management>WEB Directory**.



File	Size (bytes)	Compressed Size (bytes)
<a href="#">fwaccess.asp</a>	547	376
<a href="#">fwcfg.ASP</a>	3649	1481
<a href="#">fwcfg.htm</a>	1301	839
<a href="#">fwenables.asp</a>	2999	1476
<a href="#">fwj.js</a>	771	419
<a href="#">fwlog.asp</a>	1286	771
<a href="#">fwlog.htm</a>	474	294
<a href="#">fwlogTOP.HTM</a>	333	248
<a href="#">fwstate.asp</a>	2448	1118
<a href="#">fwtop.htm</a>	1207	828
<a href="#">GEN.ASP</a>	19124	7736
<a href="#">GOAHEAD.GIF</a>	1359	1526
<a href="#">gpscfg.asp</a>	11667	4704
<a href="#">gpsstat.asp</a>	1054	656
<a href="#">graph.js</a>	440	323
<a href="#">green_button.gif</a>	813	583
<a href="#">green_button.gif</a>	160	162
<a href="#">GREENLED.GIF</a>	534	501
<a href="#">grey_button.gif</a>	875	931
<a href="#">hotspot.asp</a>	2409	1259
<a href="#">hs_login.asp</a>	3128	1725
<a href="#">idigi.asp</a>	8928	3505
<a href="#">idigiadv.asp</a>	6701	2845
<a href="#">idigisms.asp</a>	7475	2715
<a href="#">igmpST.ASP</a>	780	570

Scroll down until you find the file **hs\_login.asp**. Click on it and scroll up until you see the default splashpage. Right click anywhere in that image and choose 'View Source'.

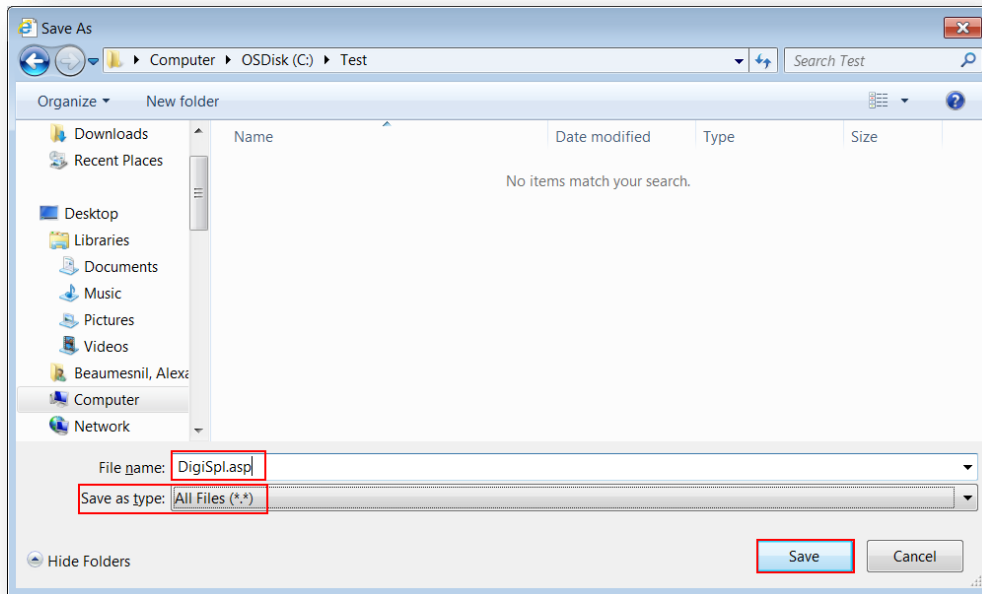


A new window will pop up (either an html editor if you have one or a web browser if you don't).



Save that file as a .asp file (example: **DigiSpl.asp**).

NOTE: Digi TransPort file system file names must be *12 characters or less (including the ".")*; typically in 8.3 format.



Reopen the .asp file either with an html editor (Notepad works fine). At about line 34 you'll see this line: `<input name="cky" value="0" type="hidden">`. This needs to be changed to: `<input name="cky" value="<%write(cky);%>" type="hidden">`.

```
19
20 params = getUrlVars (window.location.href);
21
22 if( params["login_failure"] == undefined )
23 {
24     params["login_failure"] = "0";
25 }
26 </script>
27 </head>
28 <body>
29 <form name="hotspot" action="/goform/hotspot" method="post">
30
31 <!--
32 <input type="hidden" name="hotspot_url" value="http://www.digi.com">
33 -->
34 <input name="cky" value="<%write(cky);%>" type="hidden">
35
36 <div>
37 <table style="width:100%; border="0" cellpadding="2" cellspacing="2">
38 <tbody>
39 <tr align="center">
40 <td></td>
41 </tr>
42 <tr align="center" rowspan="1"></tr>
43 </tr>
44 <tr align="center">
45 <td>This is a sample Terms and Conditions page for the <br>
46 Digi Transport Wi-Fi Hotspot functionality. <br>
47 This page can be used as a basis for a personalised Terms <br>
48 and Conditions page.<br>
```

Save the file. You now have a working file that can be manipulated anyway you need.

You can now make changes to the file as needed; i.e. the disclaimer or any GIF or JPG images that you want to add. Keep in mind that all files need to be in the 8.3 format, so any files added must be named with 12 characters or less (example: image.gif).

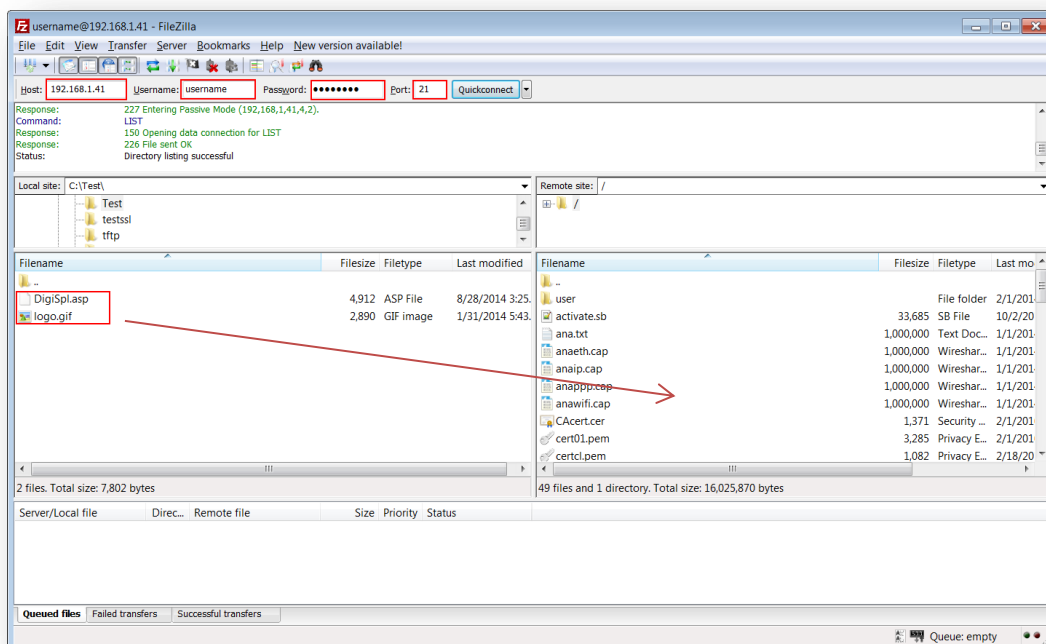
## 8.2 Change the image file

**NOTE:** Graphic types **gif** and **jpg** are supported. Other file types (e.g. png) are NOT supported. (Exceptions for gifs and jpgs are made to allow them to be accessed from the TransPort's Web server if the user has not logged in to the TransPort itself.)

The *hotspot.asp* file contains the line '**<td colspan="3" rowspan="1"></td>**'. Rename **logo.gif** as needed to the filename of the new gif file you created. Also, *remove "/images"* from address since the logo.gif is stored in the main (root) flash directory (see the example below). This is the only change to hotspot.asp needed for the images to be displayed.

## 8.3 Load new splashpage and images onto the TransPort

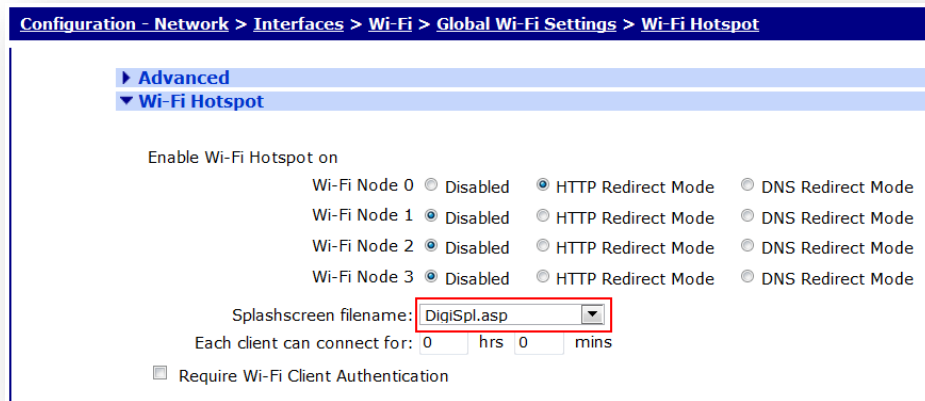
Use FileZilla or other ftp client to copy the files onto the TransPort. Windows Explorer (not Internet Explorer) works via <ftp://192.168.1.1> (assuming the Transport's LAN IP address is 192.168.1.1). You will be prompted to login to the TransPort (username and password). Drag and drop your new file (and the gif file(s) you've created) directly into the TransPort file system. They will be listed in the default (flash) directory.



Parameter	Setting	Description
-----------	---------	-------------

Host	192.168.1.23	IP Address of the TransPort router
Username	username	Username with Access Level : Super to log in to the TransPort router (default : username)
Password	password	Password for the user with Access Level : Super to log in to the TransPort router (default : password)
Port	21	Default FTP port.
DigiSpl.asp	-	Splashpage file
logo.gif	-	Image file

**Configuration-Network>Interfaces>Wi-Fi>Global Wi-Fi Settings>Wi-Fi Hotspot**



Select the drop down window called **Splashscreen filename**. Drop it down and the .asp file you loaded should appear (a reboot may be necessary if the file does not appear). Click the **HTTP Redirect Mode or DNS Redirect Mode** button for the appropriate Wi-Fi node on which the splashpage will appear.

**Apply** and **Save** configuration.

The Wi-Fi user should now be presented with the new page.



## 9 SPLASHPAGE EXAMPLE FILE

**Bold characters** are the changes made from the default hotspot.asp page.

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
  <meta content="0" http-equiv="Expires">
  <meta content="no-cache" http-equiv="Cache-Control">
  <meta content="no-cache" http-equiv="Pragma">
  <link type="text/css" href="style.css" rel="stylesheet">
  <title>Digi TransPort Terms and Conditions</title>
<script language="javascript">
var params = new Array();

function getUrlVars() {
  var vars = {};
  var parts = window.location.href.replace(/[?&]+(?:^=&+)=([^\&]*)/gi,
function(m,key,value) {
  vars[key] = unescape(value);
  });
  return vars;
}

params = getUrlVars (window.location.href);

if( params["login_failure"] == undefined )
{
  params["login_failure"] = "0";
}
</script>
</head>
<body>
  <form name="hotspot" action="/goform/hotspot" method="post">

<!--
  <input type="hidden" name="hotspot_url" value="http://www.digi.com">
-->
  <input name="cky" value="%write(cky);%" type="hidden">
  <div>
    <table style="width:100%;" border="0" cellpadding="2" cellspacing="2">
      <tbody>
        <tr align="center">
          <td></td>
        </tr>
        <tr>
          <td rowspan="1"></td>
        </tr>
        <tr align="center">
          <<td colspan="3" rowspan="1">Welcome to our Bus! <br>
If you drink then don't drive! Get home safe with us!! <br>
<br>
<br>
<br>
<br>
<br>
<br>
<br>
```

```

<br><br>
    </td>
  </tr>
  <tr>
    <td rowspan="1"></td>
  </tr>
</tbody>
</table>
<table align=center border="0" cellpadding="2" cellspacing="2">
  <tbody>
<script language="javascript">
  if( params["login_failure"] == "1" )
    {
      document.write( "<tr align='center'><td class='warning'
colspan='2'>Login attempt failed</td></tr>" )
      document.write( "<tr><td colspan='2'>&nbsp;</td></tr>" )
    }
</script>
  <tr align='center'>
    <td>
      Username:
    </td>
    <td>
      <input type="text" name="username">
    </td>
  </tr>
  <tr align='center'>
    <td>
      Password:
    </td>
    <td>
      <input type="password" name="password">
    </td>
  </tr>
  <tr>
    <td colspan="2" style="text-align: center;">
      <input name="accept" value="Accept" type="hidden">
      <input name="saccept" size="20" value="Login"
onclick="hotspot.accept.value='Accept'" type="submit">
    </td>
  </tr>
</tbody>
</table>
<div class="copyright">
  <div>
    Copyright &copy; Digi International Inc. All rights reserved.
  </div>
</div>
</form>
</body>
</html>

```