



Digi Wi-Point 3G Remote Manager

User's Guide

Version 2.0.2-5

February 2009

90001017_A

Contents



Table of Contents

ABOUT DIGI WI-POINT 3G REMOTE MANAGER.....	4
SYSTEM REQUIREMENTS	6
HARDWARE REQUIREMENTS.....	6
SOFTWARE REQUIREMENTS	6
CONFIGURATION SCENARIOS	8
INSTALLATION	9
1.1 INSTALL THE DIGI WI-POINT 3G REMOTE MANAGER SOFTWARE	9
1.2 RUN DIGI WI-POINT 3G REMOTE MANAGER SYSTEM	12
LOGIN TO DIGI WI-POINT 3G REMOTE MANAGER AND SYSTEM MANAGEMENT	13
2.1 LOGIN TO DIGI WI-POINT 3G REMOTE MANAGER.....	13
2.2 SYSTEM ADMIN LOGIN.....	14
2.2.1 LICENSE.....	16
2.2.2 REGISTER THE DIGI WI-POINT 3G REMOTE MANAGER SYSTEM	16
2.2.3 CREATE DOMAIN.....	17
2.2.4 SERVICES MANAGEMENT	19
DEVICE MANAGEMENT	20
3.1 DEVICE MANAGEMENT LOGIN.....	20
3.1.1 SORTING DEVICES	22
3.1.2 VIEW LOGS.....	22
3.1.3 MAP VIEW	23
3.1.4 TRAFFIC VOLUME.....	24
3.1.1 ADD/REMOVE DEVICES OR GROUPS	25
3.1.5.1 Add device to Digi Wi-Point 3G Remote Manager.....	25
3.1.5.2 Create a group.....	26
3.1.5.3 Moving devices to a group, or groups	27
3.1.5.4 Remove a group.....	29
3.1.5.5 Remove device from a group.....	29
3.1.5.6 Remove devices from the device list.....	29
3.1.2 ADD/REMOVE USER	29

3.1.6.1	Add User to Digi Wi-Point 3G Remote Manager	30
3.1.6.2	Changing user's password and authorization	31
3.1.6.3	Remove user.....	32
CONFIGURING DEVICES		33
4.1	BASIC FUNCTION	35
4.2	WI-FI FUNCTION	37
4.3	MOBILE FUNCTION	38
4.4	SECURITY FUNCTION	40
4.4.1	IP Filter	40
4.4.2	Port Forwarding.....	41
4.5	ADMIN FUNCTION.....	42
MANAGING DEVICES		44
5.1	RESTORING DEVICE'S FACTORY DEFAULTS SETTINGS.....	44
5.2	REBOOTING DEVICE	45
5.3	COMMITTING CONFIGURATIONS	45
5.4	UPGRADING FIRMWARE	47
5.5	UPGRADING CONFIG.....	48
MONITORING DEVICE STATUS.....		50
6.1	DEVICE OVERVIEW	50
6.2	DEVICE STATUS	51

About Digi Wi-Point 3G Remote Manager

This Digi Wi-Point 3G Remote Manager's User's Guide includes hardware requirements for Digi Wi-Point 3G Remote Manager System, configuration detail, setup information, installation instructions, domain management and device management.

Digi Wi-Point 3G Remote Manager is designed for Digi Wi-Point 3G router device management and maintenance. Digi Wi-Point 3G Remote Manager can enhance network administrator work efficiency, and is capable of handling thousands of units. The network administrator uses the Digi Wi-Point 3G Remote Manager System through the Digi Wi-Point 3G Remote Manager Console via a standard web browser. This console provides tools to easily deploy, manage, monitor, and maintain devices. The console is capable of configuring, and managing devices, as well as monitoring performance, creating event logs, and performing security management.

The two components in Digi Wi-Point 3G Remote Manager System are the system admin and the domain admin.

- The system admin component allows management of all functions in the Digi Wi-Point 3G Remote Manager System. Using the system admin the administrator can create a new domain and manage all domains in the Digi Wi-Point 3G Remote Manager System. The Digi Wi-Point 3G Remote Manager server itself can also be managed from the Digi Wi-Point 3G Remote Manager Console. Server management tasks can be started, stopped, and restarted from this console.
- The domain admin component allows administrators to manage all functions in one domain. For example, domain administrators can configure, reboot, reload, and upgrade firmware.

After installation and deployment, the Digi Wi-Point 3G Remote Manager Server allows the user access and management of devices from any location.

System Requirements

Hardware Requirements

Server hardware must meet the following minimum requirements:

- Pentium 4 computer or equivalent
- 512 MB RAM
- 300MB disk space

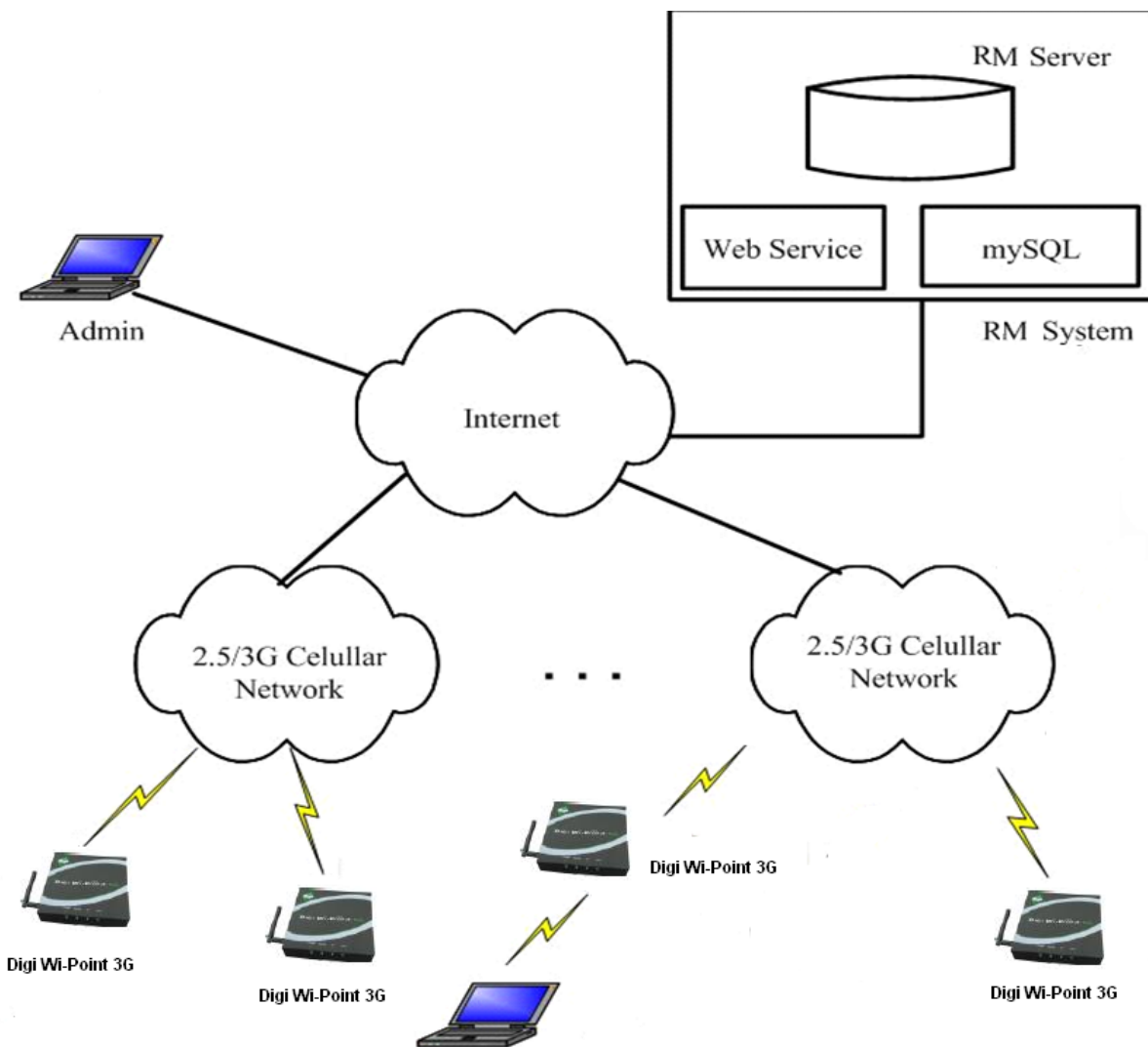
Software Requirements

- Redhat Fedora 10 only (MySQL component is required).
- Customer must be proficient in Redhat installation and operation. Digi does not provide Redhat OS-support.

Configuration Scenarios

.....

An advantage of using Digi Wi-Point 3G Remote Manager to manage Digi Wi-Point 3G devices is that each device locates the Digi Wi-Point 3G Remote Manager Server by the Server's IP address. This allows the network administrator at the Digi Wi-Point 3G Remote Manager Server's Management Console to always locate devices, even if they do not know each device's IP address. To illustrate, the following network configuration shows several Digi Wi-Point 3G wireless devices. These Digi Wi-Point 3G are all connected to the Digi Wi-Point 3G Remote Manager Server. Each device locates the Digi Wi-Point 3G Remote Manager Server by the Server IP address.



Installation

Installing Digi Wi-Point 3G Remote Manager software involves:

- Installing Digi Wi-Point 3G Remote Manager software,
- running Digi Wi-Point 3G Remote Manager, and
- starting Tomcat service.

1.1 Install the Digi Wi-Point 3G Remote Manager Software

To install the Digi Wi-Point 3G Remote Manager software on a Linux server, the user must have root privileges, then follow these steps:

1. **Power up Linux host, login system with “root” account. For example:**

```
Local host login: root \\ Use the administrator identity login
```

```
Password: *****
```

```
[root@localhost root]#
```

2. **Insert the Digi Wi-Point 3G Remote Manager software CD into the CDROM.**

3. **Mount the CDROM**

```
[root@localhost root]#mount /dev/hdc /mnt
```

4. **Change into the directory “/mnt”**

```
[root@localhost root]#cd /mnt
```

```
[root@localhost mnt]#ls \\show all files in this directory
```

```
apache-tomcat-5.5.20.tar.gz myapp.xml tomcat.script
```

```
install mysql-connector.jar TRANS.TBL
```

```
jre-1_5_0_11-linux-i586.rpm rcm-2.0.1-8.i386.rpm
```

```
jsvc server.xml
```

} \\ Digi Wi-Point 3G Remote Manager installation files

5. **Install Digi Wi-Point 3G Remote Manager**

```
[root@localhost mnt]# sh install
```

```
root@localhost mnt1# sh install
-----
1 Automatic Install(suit for first installation)
2 Install RCM
3 Update RCM
4 Install Run Environment
-----
Enter Choice: _
```



Note:

Option 1: Full installation will install all components including program environment and Digi Wi-Point 3G Remote Manager package. This option is usually closed when Digi Wi-Point 3G Remote Manager is installed for the first time.

Option 2: Reinstall Digi Wi-Point 3G Remote Manager and initiate Digi Wi-Point 3G Remote Manager. This option will reinstall Digi Wi-Point 3G Remote Manager components, and delete all old data in the database including some private data.

Option 3: Only update Digi Wi-Point 3G Remote Manager component. This option will keep all original data.

Option 4: Only install program environment including TOMCAT and JRE.

Complete the installation process according to the prompt information. For example:

`[root@localhost mnt]#Enter choice:1`

```

Enter Choice:1
clean old jre!
install jre ...
clean old tomcat!
install tomcat
fix server.xml ....
copy jsvc ...
`jsvc' -> /usr/local/apache-tomcat-5.5.20/bin/jsvc'
install tomcat startup script ...
Shutting down rcmd: [FAILED]
Stopping Tomcat: [FAILED]
clean old rcmd!
install rcmd
Stopping MySQL: [ OK ]
Starting MySQL: [ OK ]
remove old database ...
Initializing RCM database ...

##### Add user 'rcm' into mysql user table #####
Enter password: _

```

Enter the password of MySql administrator.



Note: In Linux FC10, the default password of Mysql Administrator is null.

Press the **ENTER** key.

```

Enter password:
ERROR 1396 (HY000) at line 1: Operation CREATE USER failed for 'rcm'@'%'
update version ...
[root@localhost mnt]# _

```



Note:

If the above information is encountered, it should be ignored. Typically this appears when the Digi Wi-Point 3G Remote Manager is reinstalled.

1.2 Run Digi Wi-Point 3G Remote Manager System

To start Digi Wi-Point 3G Remote Manager, start the Tomcat server (as Web Server) application and follow the instructions below:

1 Start Tomcat service

```
[root@localhost mnt]#service tomcat start
```

2 Start Mysql service

```
[root@localhost mnt]#service mysqld start
```

3 Start Digi Wi-Point 3G Remote Manager service

```
[root@localhost mnt]#service rcmd start
```

```
[root@localhost ~]# service tomcat start
Starting Tomcat:                               [ OK ]
[root@localhost ~]# service mysqld start
Starting MySQL:                               [ OK ]
[root@localhost ~]# service rcmd start
Starting rcmd:                                 [ OK ]
[root@localhost ~]#
```

Login to Digi Wi-Point 3G Remote Manager and System Management

2.1 Login to Digi Wi-Point 3G Remote Manager

Open a Web browser (IE6 recommend) and enter <https://xxx.xxx.xxx.xxx:8443> in address bar (“xxx.xxx.xxx.xxx” is the IP address or URL of Digi Wi-Point 3G Remote Manager Server). Press **ENTER**, and the Digi Wi-Point 3G Remote Manager Login page will be displayed (Figure 2-1).

Figure2- 1 Login page



There are two choices:

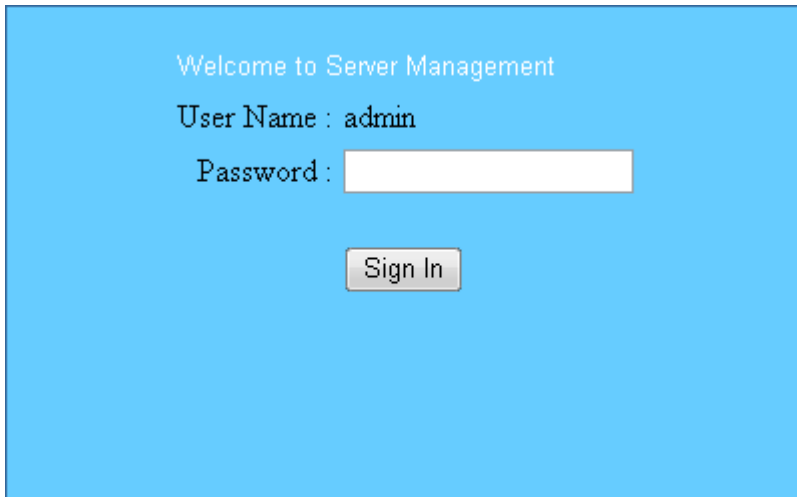
- **Server Management:** Server Management can manage all the functions in Digi Wi-Point 3G Remote Manager System. Such as creating domain, managing domains and restarting Digi Wi-Point 3G Remote Manager Service. Choose System Management if you need to add license, set up domain to manage devices.

- **Device Management:** Users can only manage devices authorized to their accounts.

2.2 System Admin Login

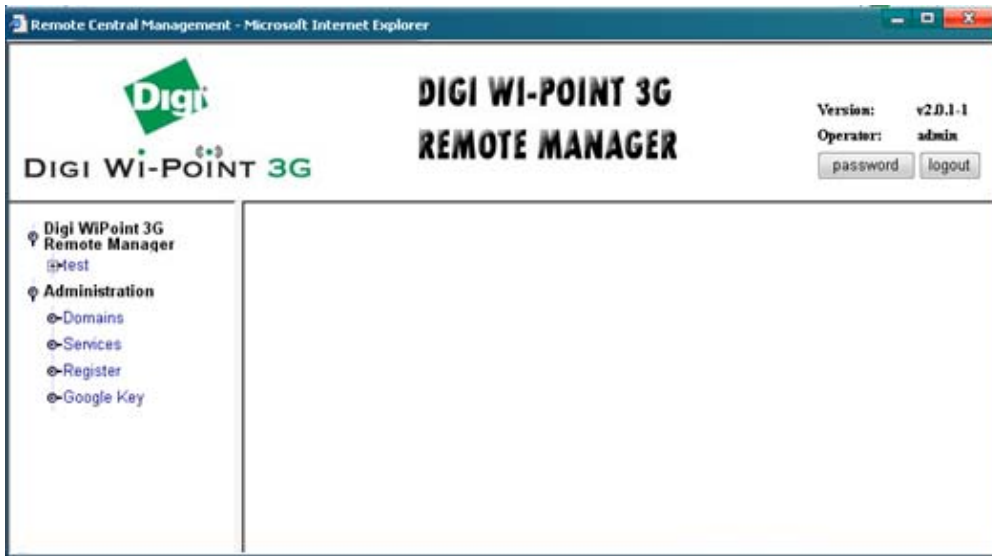
1. Login to Digi Wi-Point 3G Remote Manager web server with a system administrator account to manage all devices associated with this server.
2. Click “Server Management.” The password page will be displayed (Figure2-2).
3. Input the password (default is admin). The home page of Digi Wi-Point 3G Remote Manager web site will be displayed (Figure 2-3).

Figure2- 2 Password



Welcome to Server Management
User Name : admin
Password :

Figure2- 3 System home page



If this is the first time the Digi Wi-Point 3G Remote Manager has been used, the list of Digi Wi-Point 3G Remote Managers in the left pane is empty. To use the Digi Wi-Point 3G Remote Manager System, the system must be registered.

This page allows the following functions:

- Register the Digi Wi-Point 3G Remote Manager system
- Register the Google key
- Manage domains
- Restart Digi Wi-Point 3G Remote Manager service
- Manage devices

2.2.1 License

The Digi Wi-Point 3G Remote Manager Server registration includes three parts: **System License Code**. This license code is necessary for registration of the Digi Wi-Point 3G Remote Manager. The number of domains that can be created in a Digi Wi-Point 3G Remote Manager server is limited by this code. Obtain a license code from Digi, International by contacting your Digi representative. Refer to session “2.2.2 Register the Digi Wi-Point 3G Remote Manager System.”

■ Domain Authorized Code

When a new domain is created, the domain is unauthorized. This code restricts the number of groups, devices, firmwares and users in this domain. To authorize the domain and make it available later, a domain authorized code must be obtained from Digi, International. Refer to session “2.2.3 Creating Domain.”

■ Google key

To use the Map View function, a Google key is necessary for registration of Digi Wi-Point 3G Remote Manager.

Users can get a key from <http://www.google.com/apis/maps/signup.html> .

2.2.2 Register the Digi Wi-Point 3G Remote Manager System

This section describes how to register the Digi Wi-Point 3G Remote Manager System the first time the Digi Wi-Point 3G Remote Manager Server is used.

➤ Register the Digi Wi-Point 3G Remote Manager system

1. Click **Register** on the menu. The register page of Digi Wi-Point 3G Remote Manager web site will be displayed.
2. Enter an arbitrary username.
3. Enter the license key for your Digi Wi-Point 3G Remote Manager Server. Contact Digi, International for ordering details.
4. Click **Submit**.

Figure2- 4 Register

Register	
Register Information	
User:	<input type="text" value="test"/>
Key:	<input type="text"/>
<input type="button" value="Submit"/>	

2.2.3 Create Domain

Click **Domains** on the menu, and then select **Create New Domain** from the dropdown menu of **Actions** items.

Figure2- 5 Add Domain

Add Domain		Actions
Basic Information		---Available Actions---
Domain Name:	<input type="text" value="test"/>	
Domain Desc:	<input type="text" value="test"/>	
Devices Limit:	<input type="text" value="5"/>	
Groups Limit:	<input type="text" value="2"/>	
Firmware Limit:	<input type="text" value="3"/>	
User Limit:	<input type="text" value="3"/>	
Auto Register:	<input type="radio"/> N <input checked="" type="radio"/> Y	
Administrator Account		
User Name:	<input type="text" value="test"/>	
Password:	<input type="text" value="test"/>	
<input type="button" value="Create"/> <input type="button" value="Reset"/>		

Enter basic information and an administrator account in this page. Click **Create** and the new domain will be displayed in the domain list. This new domain status is unauthorized.

- **Basic information**

Domain Name: Domain name.

Domain Desc: Domain description (optional).

Groups Limit: The maximum number of groups in this domain.

Devices Limit: The maximum number of devices in this domain.

Firmware Limit: The maximum number of firmware in this domain.

User Limit: The maximum number of users in this domain.

Auto Register: Automatically allow or deny registration of a device in this domain.

- **Administrator account**

User name: Username for domain administration.

Password: Password for domain administration.

Figure2- 6 Domain List

Domain List		Actions					
<input type="checkbox"/>	Domain Name	Status	Max.Devices	Max.Groups	Max.Firmwares	Max.Users	Auto Register
<input type="checkbox"/>	test	Unauthorized	5	2	3	3	1

To activate this domain, a domain authorized code must be entered.

1. Click **Domain Name** to go to its management page.
2. Select **Authorize Domain** from the dropdown menu of **Actions** items to register this new domain.

Figure2- 7 License information

Register	
License Information	
Hardware ID:	3HV3CE2S
Software SN:	test
Domain Name:	test
Devices:	5
Groups:	2
Firmwares:	3
Users:	3
Register Information	
Key:	<input type="text"/>
<input type="submit" value="Submit"/>	

3. Enter Domain Authorization Code.
4. Click **Submit**.

Figure2- 8 Domain List

Domain List							Actions	----Available Actions----
<input type="checkbox"/>	Domain Name	Status	Max.Devices	Max.Groups	Max.Firmwares	Max.Users	Auto Register	
<input type="checkbox"/>	test	Authorized	5	2	3	3	1	

5. Repeat this step to create more domains.

2.2.4 Services management

Use the Services management function to for monitoring the operational status of the Digi Wi-Point 3G Remote Manager Server or for performing remote administration on the server.

Start button: Start the Digi Wi-Point 3G Remote Manager Service.

Stop button: Stop the Digi Wi-Point 3G Remote Manager Service.

Restart button: Restart the Digi Wi-Point 3G Remote Manager Service.

Figure2- 9 Services

Services List			
<input type="checkbox"/>	Services Name	Version	Status
<input checked="" type="checkbox"/>	rcmd	v1.0.2-1	Started

Chapter 3

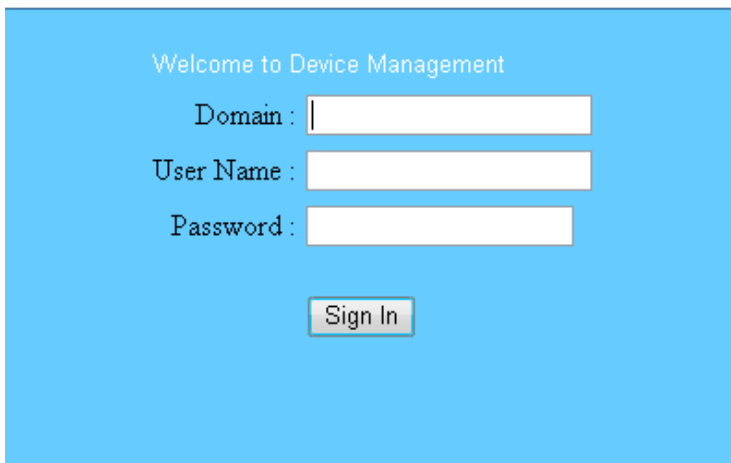
Device Management

3.1 Device Management Login

Only devices authorized to an account can be managed with the Digi Wi-Point 3G Remote Manager web server.

1. On the Digi Wi-Point 3G Remote Manager login page, click Device Management. The Device Management password page will be displayed (Figure3-1).
2. Enter the user name\password\domain.
3. Access the home page to manage devices authorized to this account (Figure 3-2).

Figure 3- 1 password



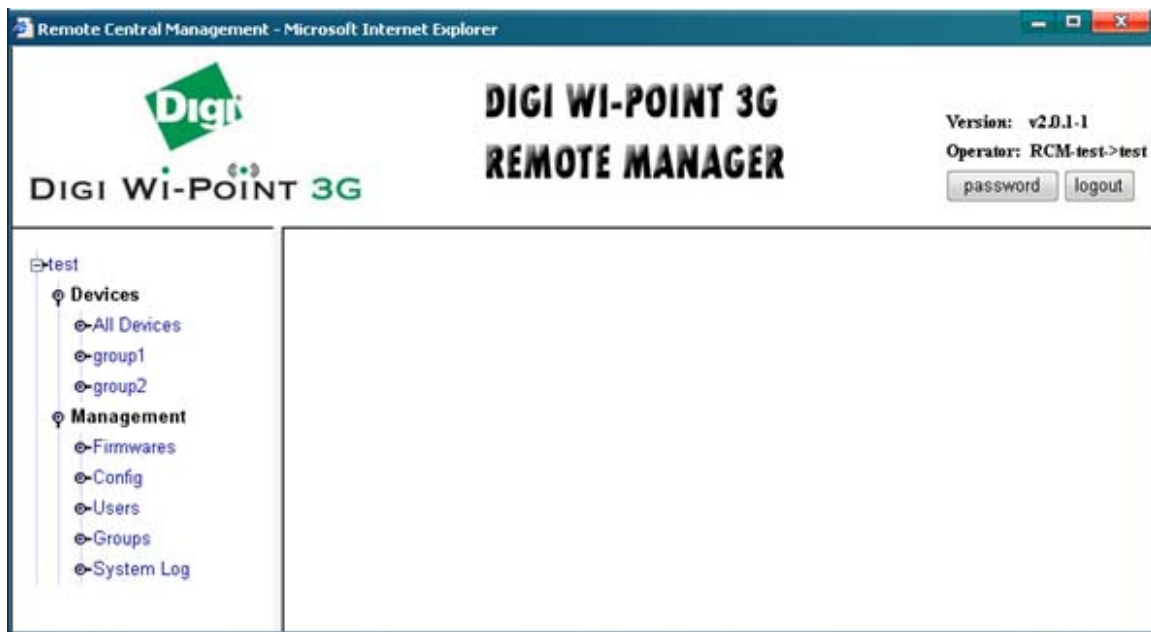
Welcome to Device Management

Domain :

User Name :

Password :

Figure 3- 2 Device Management home page



3.1.1 Sorting Devices

This section describes changing the display of the information in the **Device List**. If hundreds of devices are being managed, the device list will be lengthy. Going through the list to locate a particular device among all of the devices is inconvenient and time-consuming. This system provides two methods to sort devices.

SN: Sort devices by the **SN** numbers.

Model: Sort devices by the **Model** types.

➤ **To display devices with SN or Model**

1. Go to **All Devices** page or any **Group** page.

➤ Select one sort mode from the dropdown menu of **Actions** items, **SN or Model**.

3.1.2 View Logs

In the Digi Wi-Point 3G Remote Manager system, there are two logs, system log and device log.

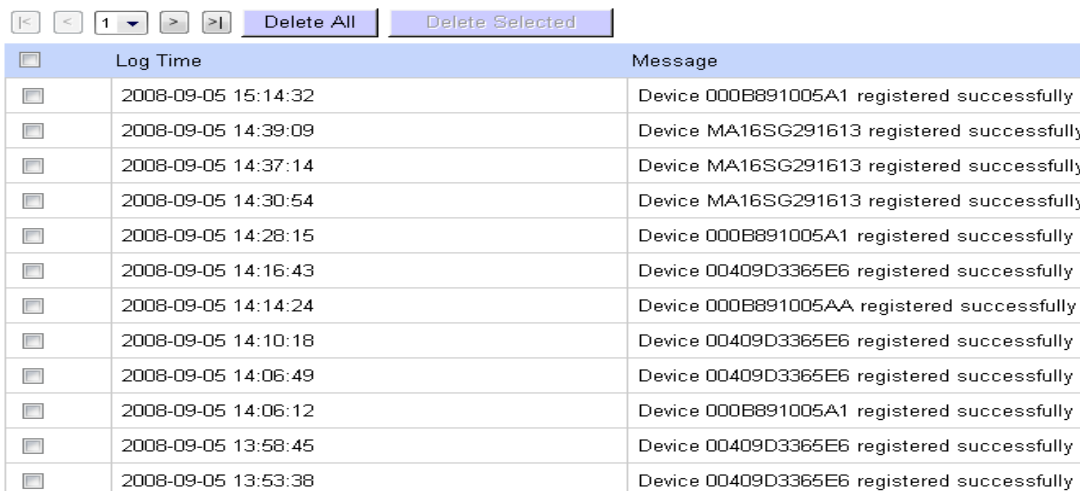
➤ **Viewing system logs**

To view logs,

1. Click **System Log** on the menu. Device connection information will be recorded in the system log.

Figure 3- 3 System Log

System Log



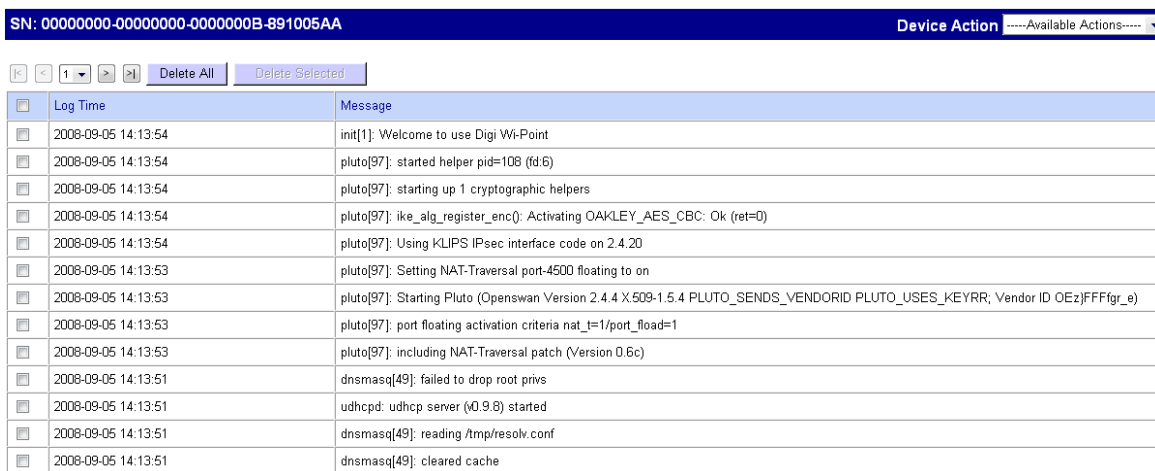
<input type="checkbox"/>	Log Time	Message
<input type="checkbox"/>	2008-09-05 15:14:32	Device 000B891005A1 registered successfully
<input type="checkbox"/>	2008-09-05 14:39:09	Device MA16SG291613 registered successfully
<input type="checkbox"/>	2008-09-05 14:37:14	Device MA16SG291613 registered successfully
<input type="checkbox"/>	2008-09-05 14:30:54	Device MA16SG291613 registered successfully
<input type="checkbox"/>	2008-09-05 14:28:15	Device 000B891005A1 registered successfully
<input type="checkbox"/>	2008-09-05 14:16:43	Device 00409D3365E6 registered successfully
<input type="checkbox"/>	2008-09-05 14:14:24	Device 000B891005AA registered successfully
<input type="checkbox"/>	2008-09-05 14:10:18	Device 00409D3365E6 registered successfully
<input type="checkbox"/>	2008-09-05 14:06:49	Device 00409D3365E6 registered successfully
<input type="checkbox"/>	2008-09-05 14:06:12	Device 000B891005A1 registered successfully
<input type="checkbox"/>	2008-09-05 13:58:45	Device 00409D3365E6 registered successfully
<input type="checkbox"/>	2008-09-05 13:53:38	Device 00409D3365E6 registered successfully

2. Clear the log by clicking **Delete All** or **Delete Selected**.

➤ View device logs

When the device is connected to the Digi Wi-Point 3G Remote Manager Server, the device can send its log messages to the Digi Wi-Point 3G Remote Manager Server so that the administrator can view, monitor, and diagnose the device remotely. Select **Log** from the dropdown menu of **Device Action** items and log information can be examined.

Figure 3- 4 Device Log



The screenshot shows a web interface for viewing device logs. At the top, there is a blue header bar with the device's serial number (SN: 00000000-00000000-0000000B-891005AA) on the left and a 'Device Action' dropdown menu on the right. Below the header, there are two buttons: 'Delete All' and 'Delete Selected'. The main content is a table with two columns: 'Log Time' and 'Message'. The table contains 13 rows of log entries, each with a checkbox in the 'Log Time' column.

Log Time	Message
<input type="checkbox"/> 2008-09-05 14:13:54	init[1]: Welcome to use Digi Wi-Point
<input type="checkbox"/> 2008-09-05 14:13:54	pluto[97]: started helper pid=108 (fd.6)
<input type="checkbox"/> 2008-09-05 14:13:54	pluto[97]: starting up 1 cryptographic helpers
<input type="checkbox"/> 2008-09-05 14:13:54	pluto[97]: ike_alg_register_enc(): Activating OAKLEY_AES_CBC: Ok (ret=0)
<input type="checkbox"/> 2008-09-05 14:13:54	pluto[97]: Using KLIPS IPsec interface code on 2.4.20
<input type="checkbox"/> 2008-09-05 14:13:53	pluto[97]: Setting NAT-Traversal port=4500 floating to on
<input type="checkbox"/> 2008-09-05 14:13:53	pluto[97]: Starting Pluto (Openswan Version 2.4.4 X.509-1.5.4 PLUTO_SENDS_VENDORID PLUTO_USES_KEYRRR; Vendor ID OEz)FFFFgr_e)
<input type="checkbox"/> 2008-09-05 14:13:53	pluto[97]: port floating activation criteria nat_=1/port_float=1
<input type="checkbox"/> 2008-09-05 14:13:53	pluto[97]: including NAT-Traversal patch (Version 0.6c)
<input type="checkbox"/> 2008-09-05 14:13:51	dnsmasq[49]: failed to drop root privs
<input type="checkbox"/> 2008-09-05 14:13:51	udhcpd: udhcp server (v0.9.8) started
<input type="checkbox"/> 2008-09-05 14:13:51	dnsmasq[49]: reading /tmp/resolv.conf
<input type="checkbox"/> 2008-09-05 14:13:51	dnsmasq[49]: cleared cache

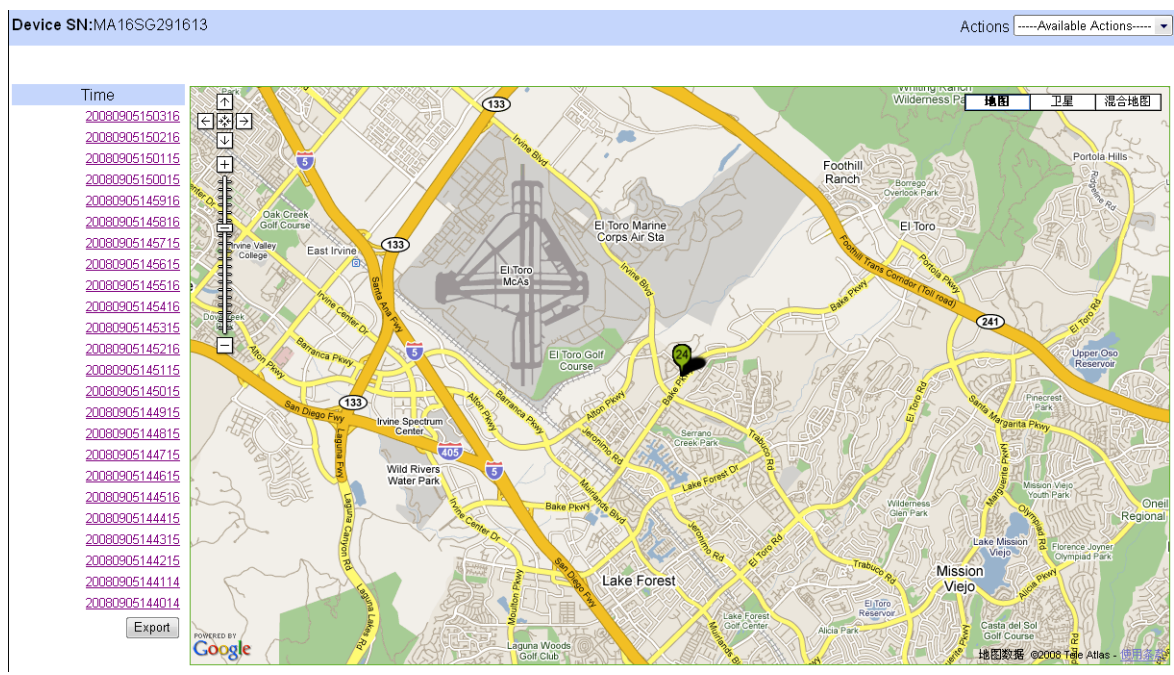
Clear the log messages by clicking **Delete All** or **Delete Selected**.

3.1.3 Map View

The GPS function in Digi Wi-Point 3G can be enabled. Currently, Digi Wi-Point 3G GPS function supports a S720 card. The Digi Wi-Point 3G mobile track will be displayed on the map when a location changes.

1. Go to **All Devices** page or any **group** page.
2. Click **Map View** from the drop down menu of **Actions** items.
3. Select the device to view.

Figure 3- 5 Map View



A user can set up GPS transfer interval in Digi Wi-Point 3G configuration page (Figure4- 1) set up GPS log records (Figure3-5), and download GPS log information.

3.1.4 Traffic Volume

1. Check throughput of every device in this page.

Figure 3- 6 Dataflow

Device List - All Devices (3/3) Actions -----Available Actions-----

Navigation: [Left Arrow] [Right Arrow] [1] [Left Arrow] [Right Arrow]

	SN	Send Bytes	Recv Bytes	Avg Send Bytes Per Day	Avg Recv Bytes Per Day
<input type="checkbox"/>	00000000-00000000-0000000B-891005A1	0	0	0	0
<input type="checkbox"/>	00000000-00000000-0000000B-891005AA	0	0	0	0
<input type="checkbox"/>	00000000-00000000-00000040-9D3365E6	716862288	16	358431144	8

[Detail] [Export]

2. Click **export** button to save traffic log information into local host.

3. Select a device.
4. Click the **detail** button to see the device traffic log information each hour.

3.1.1 Add/Remove Devices or Groups

When a device is added, by default it will be added into the **All Devices** group and be displayed in the device list. From there, the device can be removed or put into another group.. A number of groups can be created and used to organize devices. For example, create groups based on geographical locations or device types. After groups are created and devices moved into them, tasks can be performed on all the devices in the same group, rather than on each individual device. For example, the user can configure several devices and perform administrative tasks on all of them at one time.

3.1.5.1 Add device to Digi Wi-Point 3G Remote Manager

➤ **Configure Digi Wi-Point 3G Remote Manager client (MobileBridge™)**

Configure devices to support remote management. To manage Digi Wi-Point 3G through Digi Wi-Point 3G Remote Manager, configure the Digi Wi-Point 3G Remote Manager client on the devices.



Usually, there are three steps to configure Digi Wi-Point 3G Remote Manager Client on devices:

1. Enable Digi Wi-Point 3G Remote Manager.
2. Setup the Digi Wi-Point 3G Remote Manager server address or hostname.
3. Specify the domain name which the device belongs to.

➤ **Adding device to Digi Wi-Point 3G Remote Manager**

To connect a new device to Digi Wi-Point 3G Remote Manager server, there are two methods.

- If the domain is set to allow auto-register device, only enable Digi Wi-Point 3G's Remote Manager and setup the domain on the device, then the device will automatically register to this domain.

- If the domain is set to deny auto-register device, configure the device first (refer to the User's Guide of device). Then add this device to Digi Wi-Point 3G Remote Manager server manually using the following steps.
 1. Go to **All Devices** page or any **Group** page.
 2. Select **Add New Device** from the dropdown menu of **Actions** items.

Figure 3-7 Create New Device

Create New Device

Device Information	
SN:	<input type="text"/>
Name:	<input type="text"/>
GPS records:	<input type="text" value="10080"/>
Comment:	<div style="border: 1px solid gray; height: 40px; width: 100%;"></div>

3. Input the SN of the device which to be connect to Digi Wi-Point 3G Remote Manager System.
4. Click **Create** and the device will be added to the list.

A GPS log number can be set up in the GPS Number textbox.

3.1.5.2 Create a group

Users can add several groups for the devices, so that the devices are managed as a group.

Click **Groups**, and the group management page of the Digi Wi-Point 3G Remote Manager web site will be displayed.

Figure 3- 8 Groups

Group List

<input type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	group1	group1
<input type="checkbox"/>	group2	group2

Group Name :

Description :

Enter the group name and description and then click **New Group** button. The new group will appear in the group list.

3.1.5.3 Moving devices to a group, or groups

➤ Adding devices to a group

Add a device to group as follows:

1. Click **All Devices** group to go to its management page
2. Check the checkbox in front of the device which is to be added to the group.
3. Click one group that is to be added from the dropdown menu on the lower right and the device will be added to the group selected.

Figure 3- 9 All Devices

Device List - All Devices (0/3) Actions -----Available Actions-----

<input type="checkbox"/>	SN	Model	Firmware	Last Wan IP	RSSI	Status	Card Model	ESN	GPS Location
<input checked="" type="checkbox"/>	00000000-00000000-0000000B-S91005A1	Wi-Point 3G	v1.1.33-7	10.1.133.155		Disconnected	E630	352340012537480	INVALID
<input checked="" type="checkbox"/>	00000000-00000000-0000000B-S91005AA	Wi-Point 3G	v1.1.33-7	75.214.249.106		Disconnected	PANTECH USB MODEM	0X81C1419	INVALID
<input checked="" type="checkbox"/>	00000000-00000000-00000040-9D3365E6	Wi-Point 3G	v1.1.33-7	116.128.1.103		Disconnected	Sierra Wireless AirCard 555	D4D05BAD	INVALID
<input type="checkbox"/>	Check all online devices with updated configuration.								

⚠ means the device's configuration has been modified. To make the new configuration take effect, parameter submission and device reboot are required. Please remember to go ACTIONS list box to complete whole process.

➤ **Add a device to groups**

A device can be added to other groups as follows:

1. Select all devices or one group that contains the device to be added.
2. Click to the device serial number to view its management page.
3. Select “**Join/Detach Group**” option from the dropdown menu of **Device Actions** items.
4. Check the box in front of the group list.
5. Click save.

Figure 3- 10 *Join/Detach Group*

Join/Detach Group : 00000000-00000000-0000000B-891005A1		Device Action
		-----Available Actions-----
Group Name	Description	
<input checked="" type="checkbox"/> group1		
		Save Reset



Note: One device can belong to multi-groups.

➤ **To move a device from one group to another**

To move a device from one group to another use the following steps.

1. Select the group that contains the device to be moved.
2. Check the checkbox in front of the device in the device list.
3. Click the group where the device should be placed from the dropdown menu on the lower right.

Figure 3- 11 *Device List-group*

Device List - group1 (1/1)									Actions
									-----Available Actions-----
<input checked="" type="checkbox"/>	SN	Model	Firmware	Last Wan IP	RSSI	Status	Card Model	ESN	GPS Location
<input checked="" type="checkbox"/>	00000000-00000000-00000040-9D3365E6	Wi-Point 3G	v1.1.33-7	211.94.80.182		Connected	Sierra Wireless AirCard 555	D4D05BAD	INVALID
<input type="checkbox"/>	Check all online devices with updated configuration.								
<small>⚠ means the device's configuration has been modified. To make the new configuration take effect, parameter submission and device reboot are required. Please remember to go ACTIONS list box to complete whole process.</small>									Move to ... Disjoin Group Overview Export

3.1.5.4 Remove a group

To remove a group,

1. In the left pane, click **Groups**. The group management page of Digi Wi-Point 3G Remote Manager web site will be displayed.
2. Check the checkbox in front of the group in the list to select the group you want to delete.
3. Click **Delete Selected** button. This group will be deleted (Figure 3-7).

3.1.5.5 Remove device from a group

A device can be removed from a group and remain in the **All Devices** group (Figure 3-10).

1. Select the group from which you want to remove one or more devices.
2. Check the checkbox in front of the device list to select the device or devices to be removed.
3. Click **Disjoin Group**.

3.1.5.6 Remove devices from the device list

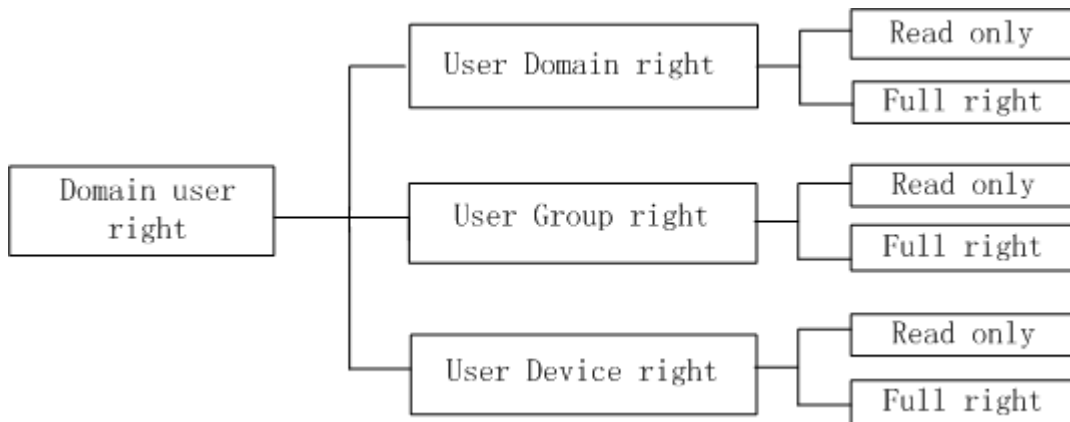
When a device is removed from **All Devices**, the device is permanently removed from the server (Figure 3-8).

1. In the **All Devices page**, select the device to be removed from the server.
2. Check the checkbox in front of the device in the list to be deleted from the group.
3. Click **Delete Selected**.

3.1.2 Add/Remove User

There are three roles of right for domain users: domain right, group right, and device right (Figure 3-11).

Figure 3- 12 Domain User privilege



Read only: The read only user is not allowed to change any configurations on domain/group/device.

Full right: The full right user has full rights to change the settings on domain/group/device.

3.1.6.1 Add User to Digi Wi-Point 3G Remote Manager

1. Click **Users** on the menu and the user management page of Digi Wi-Point 3G Remote Manager web site will be displayed (Figure 3-13).

Figure 3- 13 Users

User List		Actions
		----Available Actions----
<input type="checkbox"/>	User Name	Description
<input type="checkbox"/>	test	domain operator
<input type="checkbox"/>	test1	domain

2. Select **Create New User** from the dropdown menu of **Actions** items (Figure 3-14).

Figure 3- 14 Create New Users

Create New User		Actions
----Available Actions----		
Basic Information		
User Name:	<input type="text"/>	
Password:	<input type="password"/>	
Confirm:	<input type="password"/>	
Description:	<input type="text"/>	
Authorization Information		
Right	Read Only ▾	
Scope	<input checked="" type="radio"/> Domain Right:	test ▾
	<input type="radio"/> Group Right :	group1 ▾
	<input type="radio"/> Device Right :	▾
Create		Reset

Authorization information includes two items:

➤ Right :

Read only: If the user is limited to read only, configurations cannot be changed on Digi Wi-Point 3G Remote Manager.

Full Right: User had the full rights to change the settings.

➤ Scope :

Domain Right: User had rights to manage one domain.

Group Right: User had rights to manage one group.

Device Right: User had rights to manage one device.

3. Enter the user name, password and description. Assign a right role to user.
4. Click **Create**.

3.1.6.2 Changing user’s password and authorization

➤ **Changing password**

A new login password can be set if the old one is forgotten or for any reason needs to be changed. The new password will take effect when the user logs in to the system next time.

To change a password,

1. Click **Users**.
2. Select a **Username** (e.g. admin), and a new page will be displayed for changing password.
3. Click **change** to save the changes (Figure 3-14).

Figure 3- 15 *Edit User Properties*

User Properties	
User Name:	cynthia
Password:	<input type="text"/>
Confirm:	<input type="text"/>
Description:	<input type="text"/>

	Type	Name	Right
<input type="checkbox"/>	Group	group1	Full Right

Scope Type:

(Domain/Group/Device)Name :

Right:

➤ **Change authorization**

To change access rights:

1. Click the **User Name** to go to its management page.
2. Set authorization (Figure 3-14).
3. Choose scope type and right.
4. Click **Add Right**.

3.1.6.3 Remove user

When a user is removed from the user list, the user is permanently removed from the server.

1. Click **Users** on the menu.
2. Check the checkbox in front of the user list to select the users to delete.
3. Click **Delete selected**.

Configuring Devices

Overview

When a device is configured, its characteristics are defined. These characteristics control many aspects of device behavior. To configure a device

1. Go to **All Devices** page, or any **Group** page.
2. Click the device **SN** number.
3. Configure the device. The table below lists the types of configuration data that can be defined and provides examples of each.

Table 4-1 Configuration

Type	Function	
Digi Wi-Point 3G	Basic	<ul style="list-style-type: none"> ◆The method to use to assign the IP address ◆DHCP server settings ◆DDNS setting
	Wi-Fi	<ul style="list-style-type: none"> ◆The method to use to set the wireless LAN basic parameters ◆Wireless LAN security settings ◆Access list settings
	Mobile	<ul style="list-style-type: none"> ◆Dial mode settings ◆Keep-alive settings
	Security	<ul style="list-style-type: none"> ◆IP Filter ◆Port Forwarding

	Admin	<ul style="list-style-type: none">◆LAN/WAN Port settings◆WEB username and password settings
--	-------	--



4.1 Basic Function

Figure 4- 1 Basic

Basic Wi-Fi Mobile Security Admin

Ethernet and Wi-Fi IP Settings:
IP Address : 192.168.1.142
Subnet Mask : 255.255.255.0

GPS_LOCATION:
GPS_TRANSFER_INTERVAL : 60 Seconds

DHCP Server:
 Enable Dynamic Host Configuration Protocol (DHCP) Server
IP Addresses : 192.168.1.2 to 192.168.1.100
Lease Duration : 86400 Seconds

Static Lease Reservations :	Enabled	MAC Address	IP Address	Description
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				
<input type="checkbox"/>				

Dynamic DNS Update Settings:
 Use DynDNS.org
Choose Provider : DynDNS.org
DynDns User Name :
DynDns Password :
Host and Domain name :
Use Wildcards : Disabled

Basic part includes the primary configurations of a device.

There are four main categories of basic settings:

- 1 . LAN
- 2 . GPS-LOCATION
- 3 . DHCP server
- 4 . DDNS

● Function introduction:

■ LAN:

- **IP Address:** The IP Address of the LAN.

➤ **Subnet Mask:** The subnet mask of the LAN & WLAN.

- **GPS_LOCATION :** User can set GPS transfer interval.
- **DHCP Server:** The DHCP server shows the current DHCP IP address assigned by the device when the DHCP on the router is enabled. This setting is used to configure device Dynamic Host Configuration Protocol (DHCP) server function. Device can be used as a DHCP server for the internal LAN network. The DHCP server automatically assigns an IP address to each computer in the LAN network. To enable the device DHCP server option, configure all of PCs in the LAN network to connect to this DHCP server, and make sure there is no other DHCP server on this network.



Note:

When the DHCP server IP address range is set, it must be assured that there is no other device in the network to use the IP address located in this address range, such as printer server, file server, etc. otherwise there is risk for address conflict.

- **DDNS:** DDNS allows assignment of a fixed host and domain name to a dynamic Internet IP address. This is useful when hosting a website, FTP server, or other server behind the router. Before this feature can be used, request DDNS service at www.dyndns.com.

4.2 Wi-Fi Function

Figure 4- 2 Wi-Fi

The screenshot displays the Wi-Fi configuration page with three main sections:

- Wi-Fi LAN Settings:**
 - Wireless LAN Radio: Enabled
 - Network name: DIGIWPOINT3G
 - Wireless Channel: 6- 2.437 GHz
 - Stations Isolation: Disabled
 - Hide SSID: Enabled
- Wi-Fi Security Settings:**
 - Network Authentication: Open
 - Data Encryption: Open
 - Transmit Key: Key 1
 - Key 1: [Text Field]
 - Key 2: [Text Field]
 - Key 3: [Text Field]
 - Key 4: [Text Field]
 - PSK: Passphrase: [Text Field]
- Wi-Fi MAC Access Control List:**
 - Control Mode: Disabled
 - Rules: Enabled

Rules	MAC Address	Actions
<input type="checkbox"/>	[Text Field]	[Text Field]
<input type="checkbox"/>	[Text Field]	[Text Field]
<input type="checkbox"/>	[Text Field]	[Text Field]
<input type="checkbox"/>	[Text Field]	[Text Field]
<input type="checkbox"/>	[Text Field]	[Text Field]
<input type="checkbox"/>	[Text Field]	[Text Field]
<input type="checkbox"/>	[Text Field]	[Text Field]
<input type="checkbox"/>	[Text Field]	[Text Field]
<input type="checkbox"/>	[Text Field]	[Text Field]

There are three main categories of Wi-Fi settings:

1. Basic
2. Security
3. Access List

● **Function introduction:**

- **Basic:** This configuration is used to set the wireless LAN basic parameters.
 - **Wi-Fi Radio:** If this checkbox is set to disabled, no other parameters page is available.
 - **SSID:** The SSID must be identical for all access points in the wireless network. It is case-sensitive and must not exceed 32 characters (use any of the characters on the keyboard). For added security, change the default SSID to a unique name.
 - **Wireless Channel:** Select the appropriate channel from the list provided. All client devices in the wireless network must be broadcast using the same channel in order to function correctly.
 - **Station Isolated:** Enable this option if different client stations are being connected to the device to communicate with each other.
 - **SSID Broadcasting:** When wireless clients survey the local area for wireless networks, they will detect the SSID broadcast by the Router. To broadcast device's SSID, keep the default setting checked. If the device SSID, should not be broadcast, select Disabled.
- **Security:** This configuration is used to set wireless LAN security parameters.
 - **Network Authentication:** Select Network Authentication mode from the dropdown menu.
 - **WEP:** There are two levels of WEP encryption security, 64-bit and 128-bit. The bigger encryption bit number used, the more secure the wireless network is. However, the transmission speed is sacrificed at higher bit levels WEP security.
 - **Key Index (for transmit):** Select WEP key (1-4) to determine which key will be used during the data transmission.

Access List: This configuration is used to set the station connection control to assure the wireless network secure. This configuration assures the communication security in Wi-Fi network through encryption and authentication. It allows or denies special station connection in the Wi-Fi network.

4.3 Mobile Function

Figure 4- 3 mobile

Basic Wi-Fi Mobile Security Admin

PPP:

MTU :

MRU :

Mobile Settings:

Connect Mode : Auto

Re-establish connection when no data is received for a period time
Inactivity timeout : 15 seconds (60-86400)

Hard reset the mobile interface after the following number of consecutive failed connections.
Failed Connections : 2 (2-255)

Power-cycle the device after the following number of consecutive failed connections.
Failed Connections : 3 (2-255)

Submit Reset

There are two main categories of Mobile settings:

1. PPP Options
2. Connection Settings

● **Function introduction:**

- **PPP Options:** There are some advanced settings for the PPP dial up: the MTU and MRU. Unless the user is familiar, leave this option empty or follow the instructions from a network operator.
- **Connection Settings:**
 - **Auto:** This option enables a device to automatically dial to the Internet each time it is powered on. This keeps the device connected to the Internet, even if the connection is idle.
 - **Dial-On-Demand:** When Connect mode is set to Dial-On-Demand, the device will disable and keep alive automatically. The device can be configured to automatically disconnect from the internet after a specified period of inactivity (Max Idle Time). If the internet connection has been terminated due to inactivity, Dial-on-Demand enables a device to automatically re-establish the internet connection when needed again. The number of seconds the device should stay connected can be specified by the user.
 - **Manual:** In the Manual mode, the device will not make the internet connection when the device is powered up. To establish the cellular connection, use the client software found in the CD or on the web configuration page.

- **Keep-alive:** This option can detect whether the WWAN connection is in good status. When the WWAN connection is abnormal, it will be detected and the router will try to reconnect automatically. When the system is still abnormal, the modem will be restarted. After consecutively restarting for several (configurable) times, if the system still could not turn well, the router will reboot itself automatically.

4.4 Security Function

There are two main categories of Security function:

1. IP Filter
2. Port Forwarding

4.4.1 IP Filter

Figure 4- 4 IP Filter

The screenshot shows the IP Filter configuration interface. At the top, there are navigation tabs: Basic, Wi-Fi, Mobile, Security (selected), and Admin. Below the tabs, there are two sub-tabs: IP Filter and Port Forwarding. The main content area is titled 'IP Filter' and contains the following elements:

- Default Action:** A dropdown menu set to 'Allow'.
- Table of Filter Rules:** A table with columns: Selected, Hosts, Destination, Service, Action, and Enabled. It lists several rules, all with 'Drop' as the action and '0:65535(All)' as the service.
- Rule Edit Section:**
 - Enable this rule
 - Network Traffic of the following Services:** A dropdown menu set to 'Custom'.
 - Protocol:** A dropdown menu set to 'TCP'.
 - Port Range:** Input fields for '0' and '65535' with '(0-65535)' next to it.
 - Network Traffic from the following network:**
 - Interface:** A dropdown menu set to 'LAN'.
 - Address:** A dropdown menu set to '*'.
 - Input fields for '0.0.0.0' and '0'.
 - Network Traffic to the following network:**
 - Interface:** A dropdown menu set to 'WAN'.
 - Address:** A dropdown menu set to '*'.
 - Input fields for '0.0.0.0' and '0'.
 - Action:** A dropdown menu set to 'Block'.
 -

● Function introduction:

IP Filter is one of the most important functions of device firewall. The IP Filter of the firewall in the device has many access rules. Maintain these rules with the operations of **Add** and **Delete**.

Each rule consists of the following parameters:

- **Action:** There are two **Action** options: Drop or Pass. **Drop** means the data packet which matches this rule will be blocked by firewall. **Pass** means the data packet which matches this rule will be passed by firewall.
- **Service:** This parameter indicates the service type of this rule including the system default services and user defined services.
- **Source:** This parameter indicates the IP addresses range of data source.
- **Destination:** This parameter indicates the IP addresses range of destination.
- **Enable this rule Checkbox:** Enable or disable a rule by checking or not checking this box.

4.4.2 Port Forwarding

Figure 4- 5 Port Forwarding

The screenshot shows a web interface for configuring port forwarding. At the top, there are tabs for 'Basic', 'Wi-Fi', 'Mobile', 'Security', and 'Admin'. The 'Security' tab is selected, and the page title is 'Port Forwarding'. Below the tabs, there is a table with the following columns: Selected, Interface, Protocol, Ext.port, NAT IP, Int.port, and Enabled. The table contains eight rows, all with 'wan' as the interface, 'All' as the protocol, and '0' for both external and internal ports. The 'Enabled' column has checkboxes, with the first one checked. Below the table is a 'Rule Edit' section with the following fields: 'Enable this rule' (checkbox), 'Protocol' (dropdown menu set to 'TCP'), 'External port' (input field with '0'), 'Forward To Internal IP Address' (input field with '0.0.0.0'), and 'Forward To Internal port' (input field with '0'). A 'Submit' button is located at the bottom of the 'Rule Edit' section.

Selected	Interface	Protocol	Ext.port	NAT IP	Int.port	Enabled
<input checked="" type="radio"/>	wan	All	0	0.0.0.0	0	<input checked="" type="checkbox"/>
<input type="radio"/>	wan	All	0	0.0.0.0	0	<input type="checkbox"/>
<input type="radio"/>	wan	All	0	0.0.0.0	0	<input type="checkbox"/>
<input type="radio"/>	wan	All	0	0.0.0.0	0	<input type="checkbox"/>
<input type="radio"/>	wan	All	0	0.0.0.0	0	<input type="checkbox"/>
<input type="radio"/>	wan	All	0	0.0.0.0	0	<input type="checkbox"/>
<input type="radio"/>	wan	All	0	0.0.0.0	0	<input type="checkbox"/>
<input type="radio"/>	wan	All	0	0.0.0.0	0	<input type="checkbox"/>

Rule Edit:

Enable this rule

Protocol : TCP

External port : 0

Forward To Internal IP Address: 0.0.0.0

Forward To Internal port : 0

Submit

● Function introduction:

This feature allows forward incoming traffic to be received on certain ports to devices behind the router in order to allow the user access to servers behind the NAT from the internet. This feature allows a web server, mail server,

FTP server, or DNS to be set on the LAN and accessed from the internet. Each item consists of the following parameters:

- **Interface:** This parameter indicates which interface of the device will implement this port Map rule. In most cases the interface should be WAN.
- **Protocol:** This parameter indicates which protocol will implement this port forwarding rule. Possible protocols are: TCP, UDP and TCP/UDP.
- **External port:** This parameter indicates the port for public access.
- **NAP IP:** This parameter indicates the IP address of the internal host which wants to provide service to the outside.
- **Internal port:** This parameter indicates the service port of internal host.

4.5 Admin Function

The management username\password and management port can be changed on this page.

Figure 4- 6 Admin

Basic Wi-Fi Mobile Security Admin

WebGUI:

Port : 80

User Name : root

Password : dbps

Enable management from WAN

Use Port: 8080

Client-Initiated Management Connection:

Enable Remote Management and Configuration using a client-initiated connection

Server Address : 124.193.95.51

Domain : 124.193.95.51

Submit Reset

● Function introduction:

- **Username:** Username for device web administration. The default username is root.
- **Password:** Password for device web administration. The default password is dbps.

- **WAN port:** The service port for HTTP. A user does not normally need to modify this value. To allow someone to manage the device from WAN, check **Allow Manage device from WAN**, and modify the port value.

Managing Devices

Overview

This chapter describes how to perform administrative tasks such as:

- Restoring one or some device factory default settings
- Rebooting one or more devices
- Committing configurations
- Upgrading one or more device firmware
- Upgrading one or more device configurations

5.1 Restoring device's factory defaults settings

Device manufacturers ship devices with some configuration settings already defined. Device factory defaults can easily be restored if needed.

➤ **To restore factory defaults:**

1. Go to the All **Devices** page or any **group** page. In the Device list, select one or more devices for which to restore factory defaults.
2. Click the **Factory Defaults** option from the dropdown menu of **Actions** items. These devices will be reloaded.

Reload operation restores the device configuration to factory defaults.



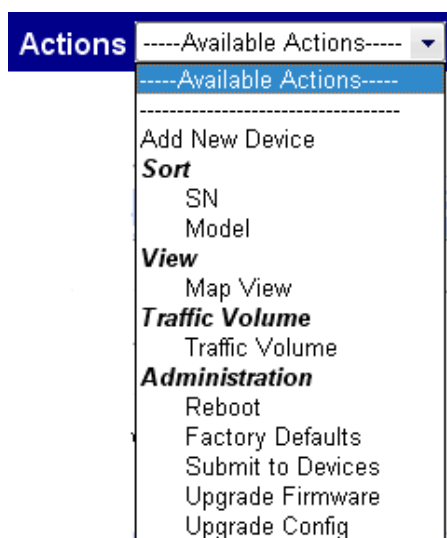
Note: If the device has been reloaded, it will be disconnected from Digi Wi-Point 3G Remote Manager.

5.2 Rebooting device

➤ **To reboot device:**

1. Go to the **All Devices** page or any **group** page.
2. Select one or more devices to reboot.
3. Click **Reboot** from the dropdown menu of **Actions** items (Figure 5-1).

Figure 5- 1 Actions



5.3 Committing Configurations

Submit to device operation saves configuration changes. To change a device configuration, click **Submit to Device**.

➤ **To make device configurations effective:**

1. Change device configuration.(refer to chapter 4)
2. Click **Submit** in device configuration page.
3. Click **Submit to device** option from the dropdown menu of **Actions** items in device configuration page.
4. Click **Reboot** option from the dropdown menu of **Actions** items.



Note: After device configurations have been changed, click the **Submit to device** option. The new configuration will take effect after the device has been rebooted.

5.4 Upgrading Firmware

When a new firmware version becomes available, download and save it on the Digi Wi-Point 3G Remote Manager server. More than one device can be upgraded.

➤ Download firmware:

1. Download the firmware to local host.
2. Click **firmware**.
3. Click **browse** button to find the file in local file system.
4. Click the **upload** button. To upload the firmware to Digi Wi-Point 3G Remote Manager server. This firmware will show at firmware list (Figure 5-2).

Figure 5-2 Add new firmware version

The screenshot shows the 'Firmware List - Wi-Point' interface. At the top right, there is a 'Model' dropdown menu with the text '----Available Model----'. Below this is a table with three columns: 'File Name', 'Description', and 'Upload Time'. The table contains three rows of firmware data. Below the table is a 'Delete Selected' button. At the bottom, there is a form for adding new firmware with fields for 'New Firmware' (with a '浏览...' button), 'Description', and an 'Upload' button.

<input type="checkbox"/>	File Name	Description	Upload Time
<input type="checkbox"/>	WIPOINT-firmware-v1.1.33-9.bin_1		2008-09-10 17:01:18
<input type="checkbox"/>	WIPOINT-firmware-v1.1.33-7.bin		2008-09-10 17:21:13
<input type="checkbox"/>	WIPOINT-firmware-v1.1.33-10.bin		2008-09-11 09:55:23

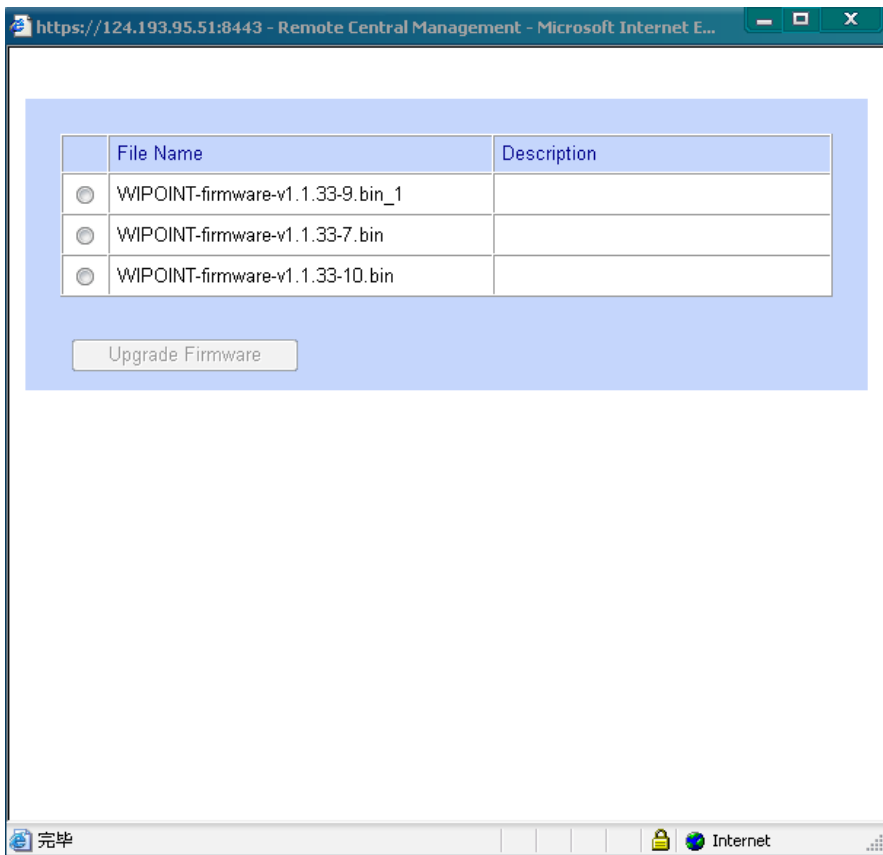
New Firmware :

Description :

➤ To update device firmware

1. In **All Devices** page or any **Group** page, select one or more devices to upgrade.
2. Click **Upgrade Firmware** option from the dropdown menu of **Actions** items. The upgrade firmware page opens:

Figure 5- 3 Upgrade firmware



1. Select the firmware version.
2. Click **Upgrade Firmware**.

5.5 Upgrading Config

The user can download the config file to Digi Wi-Point 3G Remote Manager Server, then use the config file to upgrade one or more devices at the same time.

➤ Download config:

1. Click **config** on the menu.
2. Click **browse** button to find the config file in local file system.
3. Click the **upload** button. To upload the config file to Digi Wi-Point 3G Remote Manager server. This config file name will show at firmware list (Figure 5-4).

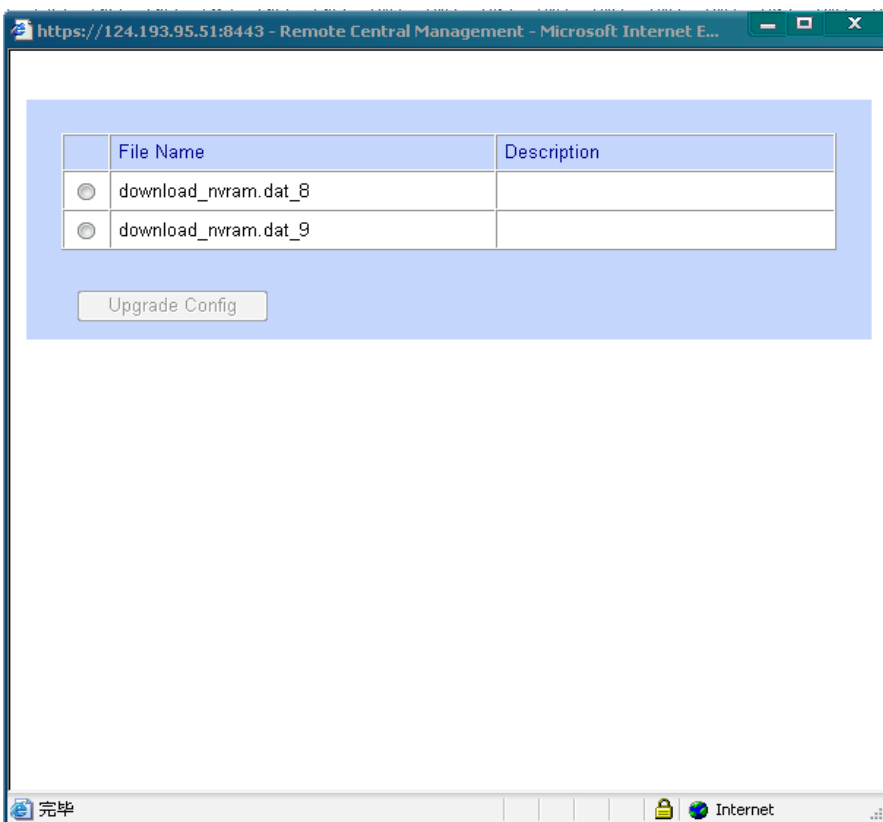
Figure 5- 4 Add config file



➤ **To update device config**

1. In **All Devices** page or any **Group** page, select one or more devices to upgrade.
2. Click **Upgrade Config** option from the dropdown menu of **Actions** items and the upgrade config page will open:

Figure 5- 5 Upgrade config



1. Select the config file.
2. Click **Upgrade Config**.

Monitoring Device Status

Overview

The Device Management application gives quick access to detailed state and statistics about a device, such as:

- Device overview
- Network settings
- Wireless LAN settings
- DHCP assign status

Device Management also allows monitoring of the device connection.

6.1 Device overview

➤ **To view an overview of statistics about a device:**

1. Go to **All Devices** page or any **Group** page.
2. Select one **SN** number.
3. Click **Overview**. The device overview information will be display.

Figure 6- 1 Device overview

Basic Information	
Model:	Wi-Point 3G
Firmware:	v1.1.33-7
Name:	<input type="text" value="null"/>
GPS records:	<input type="text" value="0"/>
Comment:	<input type="text" value="null"/>

Status Information	
Status:	Connected
Boot Duration:	7 minutes, 33 seconds
From IP:	220.205.41.160

6.2 Device status

When monitoring a device state, quick access to information about the device connection status is required.

The status page includes four submenus:

- ✓ Global(Figure 6-2)
- ✓ I/F(Figure 6-3)
- ✓ DHCP(Figure 6-4)

➤ **To view a device's connection status:**

1. Select **Status** from the dropdown menu of **Device Action** items.
2. Enter the status page. See details of a device through its **Status** page.

Figure 6- 2 Global

The screenshot displays the 'Global' status page for a device. At the top, the device's SN is 00000000-00000000-00000040-9D3365E6. The 'Device Action' dropdown menu is set to 'Available Actions'. Below the navigation tabs (Global, I/F, DHCP), there is a 'Query Status' button. The main content area is a table titled 'Device Properties' with the following data:

Device Properties	
Boot Duration:	10 minutes, 14 seconds
Memory Usage:	47% [6522306B]/[13877248B]
MAC Address:	00:40:9D:33:65:E6
LAN IP:	192.168.1.142/255.255.255.0
Wi-Fi Radio:	On
Wi-Fi SSID:	chenlj
WWAN IP:	220.205.41.160
WWAN Module:	Sierra Wireless AirCard 555
Signal Strength:	31

Figure 6- 3 I/F

SN: 00000000-00000000-00000040-9D3365E6 Device Action -----Available Actions-----

Global I/F DHCP Query Status

WAN Properties	
IP Address:	220.205.41.160
Netmask:	255.255.255.255
In/out packets:	161/167

LAN Properties	
MAC Address:	00:40:9D:33:65:E6
IP Address:	192.168.1.142
Netmask:	255.255.255.0
In/out packets:	120/77

Figure 6- 4 DHCP

SN: 00000000-00000000-00000040-9D3365E6 Device Action -----Available Actions-----

Global I/F DHCP Query Status

Station MAC	IP Address	Hostname	Remain Time
00:19:D2:B5:FE:69	192.168.1.2	tg-edaf9706f411	23 hours, 48 minutes, 34 seconds



Note: If the **status** information does not display normally, press **Query Status**.