



Backhaul Selection and Configuration Manual

On-Ramp Wireless Confidential and Proprietary. This document is not to be used, disclosed, or distributed to anyone without express written consent from On-Ramp Wireless, Inc. The recipient of this document shall respect the security of this document and maintain the confidentiality of the information it contains. The master copy of this document is stored in electronic format, therefore any hard or soft copy used for distribution purposes must be considered as uncontrolled. Reference should be made to On-Ramp Wireless, Inc. to obtain the latest revision.

On-Ramp Wireless, Inc.
10920 Via Frontera, Suite 200
San Diego, CA 92127
U.S.A.

Copyright © 2016 On-Ramp Wireless, Inc.
All Rights Reserved.

The information disclosed in this document is proprietary to On-Ramp Wireless, Inc. and is not to be used or disclosed to unauthorized persons without the written consent of On-Ramp Wireless, Inc. The recipient of this document shall respect the security of this document and maintain the confidentiality of the information it contains. The master copy of this document is stored in electronic format, therefore any hard or soft copy used for distribution purposes must be considered as uncontrolled. Reference should be made to On-Ramp Wireless, Inc. to obtain the latest version. By accepting this material the recipient agrees that this material and the information contained therein is to be held in confidence and in trust and will not be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of On-Ramp Wireless, Inc.

On-Ramp Wireless, Inc. reserves the right to make changes to the product(s) or information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis.

This document contains On-Ramp Wireless, Inc. proprietary information and must be shredded when discarded.

This documentation and the software described in it are copyrighted with all rights reserved. This documentation and the software may not be copied, except as otherwise provided in your software license or as expressly permitted in writing by On-Ramp Wireless, Inc.

Any sample code herein is provided for your convenience and has not been tested or designed to work on any particular system configuration. It is provided "AS IS" and your use of this sample code, whether as provided or with any modification, is at your own risk. On-Ramp Wireless, Inc. undertakes no liability or responsibility with respect to the sample code, and disclaims all warranties, express and implied, including without limitation warranties on merchantability, fitness for a specified purpose, and infringement. On-Ramp Wireless, Inc. reserves all rights in the sample code, and permits use of this sample code only for educational and reference purposes.

This technology and technical data may be subject to U.S. and international export, re-export or transfer ("export") laws. Diversion contrary to U.S. and international law is strictly prohibited.

RPMA® (Random Phase Multiple Access) is a registered trademark of On-Ramp Wireless, Inc.

Other product and brand names may be trademarks or registered trademarks of their respective owners.

Backhaul Selection and Configuration Manual

010-0032-00 Rev. A

January 26, 2016

Contents

1 Introduction	1
1.1 Roles for Registering the AP	1
1.2 General Prerequisites.....	1
1.3 References	1
2 LAN Backhaul.....	2
2.1 Networking Prerequisites.....	2
2.2 Connecting a Computer to the Access Point	2
2.3 Configuring the Access Point.....	2
2.4 Optional: LAN with VPN Tunnel to Remote RPMA Network	4
3 Cellular Modem Backhaul	5
3.1 Modem Selection and Ordering Process.....	5
3.2 Basic Network Configuration	6
3.3 Mobile Configuration for a CDMA/1xRTT/EVDO Carrier.....	13
3.4 Mobile Configuration for a GSM/UMTS/HSPA Wireless Carriers.....	19
3.5 Basic Security Settings.....	23
3.6 Port Forwarding Configuration Process	25
3.7 Customer-Owned Modem Backhaul Requirements.....	26
3.8 Installation and Validation Process	27
4 Connecting the AP to the RPMA Network	28

Revision History

Revision	Release Date	Change Description
A	April 30, 2015	Initial release.

DRAFT

1 Introduction

The purpose of this document is to guide customers in configuring the On-Ramp Wireless Access Point (AP) with various types of backhaul including how to use the AP webpage for configurations and/or the backhaul component of the AP. This document also covers LAN and cellular modem networks.

1.1 Roles for Registering the AP

There are two roles involved in registering the AP:

■ AP Installation Network Operator

Responsible for the network routing and forwarding rules of the AP so that the AP is accessible to the RPMA Network Operator.

■ RPMA Network Operator

Responsible for registering the AP to the RPMA network and to validate that the RPMA network has access to all of the necessary ports on the AP.

These roles may or may not be the responsibility of the same company and/or the same individual.

NOTE: This guide pertains mainly to the responsibilities of the AP Installation Network Operator. For details relating to the responsibilities of the RPMA Network Operator, refer to the EMS User Guide (010-0107-00).

In most scenarios, these two parties must communicate with one another to validate the connections. At the end of this process, the AP will wirelessly connect endpoint devices to the backend RPMA network. For any questions and/or additional support, contact support@onrampwireless.com.

1.2 General Prerequisites

- The AP Installation Network Operator must have a PC that can access the On-Ramp Wireless AP website and the cellular modem website, if applicable. If the AP Installation Network Operator does not have access to either of these websites, then the AP Installation Network Operator must contact his/her company's network administrator to obtain access.**
- The AP should already be powered on via the Power-over-Ethernet (PoE) connection.**
- The AP should already be set up with both the GPS cable and the RF antenna.**
- The RPMA Network Operator must have a user account with at least 'Operator' permissions on the Element Management System (EMS) website.**

1.3 References

Related and relevant documents for this manual are as follows:

- AP Deployment Guide (010-0021-00)**
- EMS Operator Guide (010-0107-00)**

2 LAN Backhaul

Using a LAN backhaul requires the AP to be on a local private network and, in most cases, will be physically connected to a private network.

NOTE: If the LAN AP will be connected to a remote RPMA network, then additional steps are required to set up a VPN tunnel or routing rules between the two separate networks. The method is dependent on the network security policy of the RPMA backend network entity.

2.1 Networking Prerequisites

Before configuring the AP, the following network information must be obtained from your Network Administrator:

- Static IP address to assign to the AP
- Subnet Mask
- Default Route IP address
- DNS server(s) host name(s) or IP address(es)
- NTP server(s) host name(s) IP address(es)

2.2 Connecting a Computer to the Access Point

Before configuring the AP, a computer must be physically connected to the AP via an Ethernet cable. The following steps describe how to connect a computer to the AP:

1. Configure your computer's wired Ethernet connection to:
 - a. IP address: 192.168.1.2
 - b. Subnet Mask: 255.255.255.0
2. Connect the computer to the On-Ramp Wireless cabinet switch
3. Power on the AP via the PoE connection
4. Open a web browser and enter the following information:
 - a. <https://192.168.1.1>
 - b. username = admin
 - c. password = onramp

At this point the AP web page will load in the web browser.

2.3 Configuring the Access Point

After logging into the AP, do the following:

1. Select the **Admin** link in the upper right side.



2. Select the **Network** link in the upper right side.



3. Enter the information obtained in section 2.1, into the fields indicated below.

- a. The static IP address in the **IP Address** field
- b. The Subnet Mask in the **Netmask** field
- c. The default route IP address in the **Default Router** field
- d. The DNS server(s) in the **DNS Servers** field
- e. The NTP server(s) in the **NTP Servers** field

3.4. Select **Save** button.

3.5. Select **Reboot Access Point** button.



5.6. Reopen the web browser and navigate to the AP using the newly assigned static IP address.

6.7. If primary settings are good, optionally disable secondary (to avoid any IP address collisions).

The screenshot shows the IPv4 Settings page. The 'Manual (Static IP)' tab is selected. Under 'Wired Interfaces', there are two sections: 'Primary (eth0)' and 'Secondary (eth0:0)'. The 'Secondary' section has three input fields (IP Address, Netmask, Default Router) which are highlighted with a red border. There is also a checked checkbox for 'Disable Secondary Interface?'. Other settings shown include Ethernet Speed (Auto), Duplex Mode (Auto), Ethernet MTU (1500), DNS Servers (10.50.4.252), and NTP Servers (10.50.4.252). A 'Save' button is at the bottom.

7-8. If primary settings are bad, select 'Skip rollover to Secondary,' change primary settings and reboot the AP. If the AP is rebooted with incorrect primary interface settings, it can still be accessed using the old settings using the secondary interface.

IPv4 Settings	
Wired Interfaces: click here for help	Automatic (DHCP) Manual (Static IP)
	Primary (eth0) Secondary (eth0:0)
IP Address	<input type="text" value="10.50.5.36"/>
Netmask	<input type="text" value="255.255.252.0"/>
Default Router	<input type="text" value="10.50.4.1"/>
<input checked="" type="checkbox"/> Skip rollover to Secondary?	

8-9. After successfully navigating to the AP, the configured static IP is then validated

- 9-10. Validate the NTP configuration by observing the correct time under the firmware build stamp. If the date displays January 1st, 1970, then there are three possible causes:
- The NTP server is not configured correctly on the AP website.
 - The network routing rules between the AP and the NTP server are blocking connectivity.
 - The NTP server is not functioning correctly.



10-11. Log out of the AP web page and unplug the AP from the computer

11-12. Refer to [Chapter 4: Connecting the AP to the RPMA Network](#).

2.4 Optional: LAN with VPN Tunnel to Remote RPMA Network

The AP Installation Network Operator should follow this section only if connecting an AP from a private office network to a remote external, public-facing RPMA network. This connectivity depends on the security policy of the hosted RPMA network as well as the back office for the AP. For example, the On-Ramp Wireless Hosted environment only supports point-to-point VPN connectivity between a remote LAN AP to the On-Ramp Wireless Hosted RPMA network. Please request VPN tunnel information via support@onrampwireless.com.

3 Cellular Modem Backhaul

This chapter provided information for Access Points that will reside on the public internet with the use of a 3G/4G modem as its default router. The use of a public internet modem is rated as the most convenient method for connecting an AP to a public facing RPMA Network. This chapter describes how to select an appropriate backhaul and how to configure the modem.

AP backhaul modem selection and ordering is a step-by-step process. Read each step carefully before making a selection. The following steps provide a brief overview of the process:

1. Contact a carrier and set up a plan.
2. Select a modem.
3. Order and receive the modem.
4. Configure and validate a modem.
5. Install a modem with an AP at the site. (Staging the AP is recommended)
6. Validate modem operation through the AP.

3.1 Modem Selection and Ordering Process

1. Contact a carrier (a list is provided below) who can provide the best possible coverage for the desired location(s) of your remote AP(s). The carrier can give details as to the quality and technology of coverage at the desired site(s).

Also, ask the carrier for an **unrestricted, public, static IP address**. If the carrier does not assign static IP addresses, ask for a DNS named account.

The following carriers have certified the supported modems for use on their networks:

- | | |
|---|---|
| ■ AT&T Wireless (GSM) - U.S. | ■ Claro (GSM) - Peru |
| ■ Sprint (CDMA) - U.S. | ■ Vodafone (GSM) – New Zealand |
| ■ Verizon Wireless (CDMA) U.S., Puerto Rico | ■ Comcel (GSM) - Colombia |
| ■ Rogers Wireless (GSM) - Canada | ■ IDA (GSM) - Singapore |
| ■ Midwest Wireless (CDMA) - U.S. | ■ Telstra (GSM) - Australia |
| ■ Alltel Wireless (CDMA) - U.S. | ■ Telefonica Moviles (GSM) - Guatemala, El Salvador |
| ■ T-Mobile (GSM) - U.S. | ■ ICASA (GSM) - South Africa |
| ■ Cellular One (GSM) - U.S. | ■ Movistar - Panama (CDMA), Chile (GSM) |
| ■ Centennial Wireless (CDMA) - Puerto Rico | ■ Anatel (GSM) - Brazil |
| ■ Claro PR (GSM) - Puerto Rico | ■ Bell Mobility (CDMA) – Canada |
| ■ IUSACELL (CDMA) - Mexico | ■ Dalacom (CDMA) – Kazakhstan |
| ■ Entel PCS (GSM) - Chile | |

2. Select the desired modem for use with your AP. At this time, On-Ramp Wireless fully supports the following modems:

- Digi modem #: U805 3G modem
- Digi modem #: WG-21 3G/4G modem

NOTE: Selection and use of an unsupported modem may limit AP performance, and could affect your ORW product warranty. Contact ORW to discuss BEFORE using a unsupported modem.

3. Important! Order the desired modem through the manufacturer or from another vendor.

The minimum required data plan should be as follows:

- 512 kb/sec
- 5 Gb/month

3.2 Basic Network Configuration

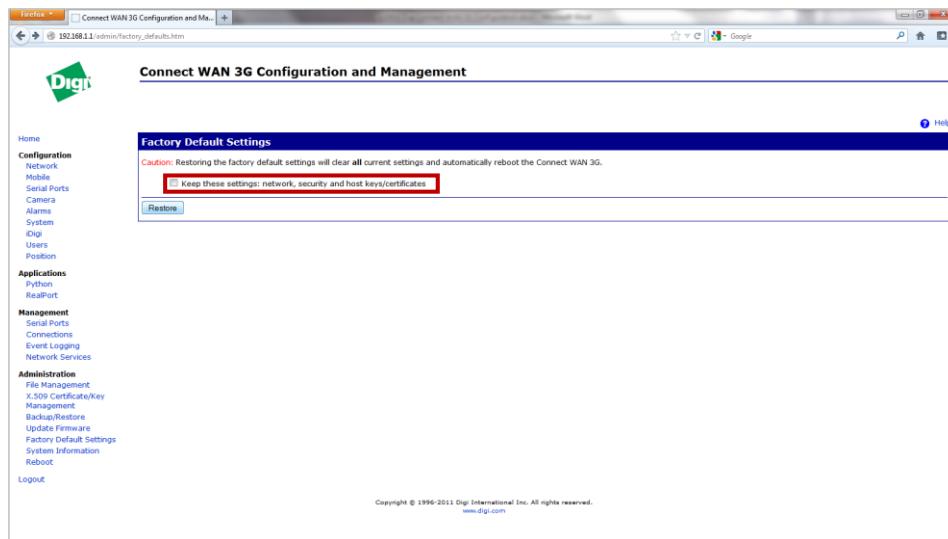
The following steps will guide you in configuring the supported modems for use with the remote AP. Refer to the sub-section below that corresponds to your modem model.

1. Configure your PC's wired Ethernet connection to:
 - a. IP Address: 192.168.1.254
 - b. Subnet Mask: 255.255.255.0
2. Open your web browser (IE, Chrome or Firefox).
3. In the URL location type <http://192.168.1.1>.

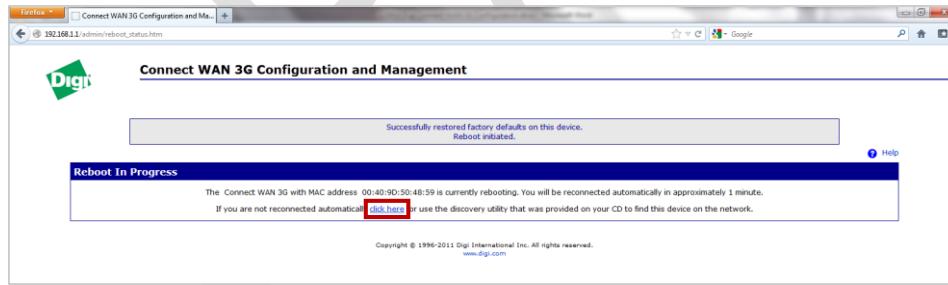


4. From the "Digi Connect WAN 3G Configuration and Management" home screen, click on the "Factory Default Settings" link on the left side of the screen under "Administration."

5. Uncheck the box for "Keep these settings: network, security and host keys/certificates" and click on the "Restore" Button.



6. Wait for the Digi Connect WAN 3G Configuration and Management home screen to appear. If you are not redirected within a few minutes, click on the "click here" link in the "Reboot In Progress" section.



7. From the “Digi Connect WAN 3G Configuration and Management, Home” screen click on the “Network” link on the left side of the screen under “Configuration.”

The screenshot shows the 'Connect WAN 3G Configuration and Management' interface. On the left, a sidebar menu includes 'Home', 'Configuration' (with 'Network' highlighted), 'Applications', and 'Administration'. The main content area displays a 'System Summary' with details like Model: Connect WAN 3G (RS232 serial), Ethernet MAC Address: 00:40:90:50:48:59, Ethernet IP Address: 192.168.1.1, Mobile IP Address: Not Connected, and Device ID: 00000000-00000000-004090FF-FF504859.

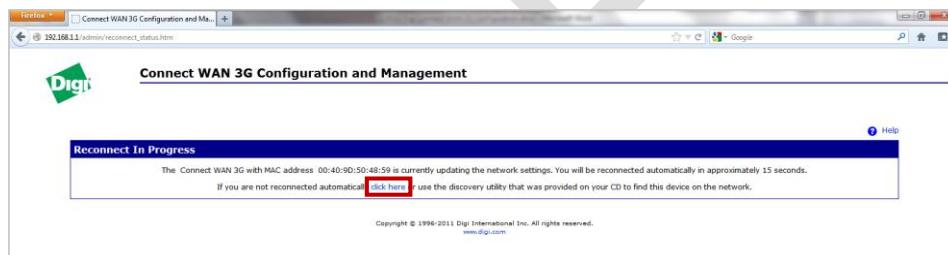
8. From the “Digi Connect WAN 3G Configuration and Management, Network Configuration” screen, changes:
 a. [Change the IP Address to 192.168.1.100.](#)
 b. [Un-check the “Enable Auto-IP address assignment” box.](#)
 c. [Click “Apply.”](#)

The screenshot shows the 'Network Configuration' screen. Under 'Ethernet IP Settings', the 'Obtain an IP address automatically using DHCP' radio button is selected, while the 'Use the following IP address' option is chosen. The IP Address is set to 192.168.1.100, Subnet Mask to 255.255.255.0, and Default Gateway to 0.0.0.0. The 'Enable AutoIP address assignment' checkbox is un-checked. Below the form, a note states: "* Changes to DHCP, IP address, and Subnet Mask may affect your browser connection." At the bottom, there is an 'Apply' button and a list of other network settings like 'DHCP Server Settings', 'Network Services Settings', etc.

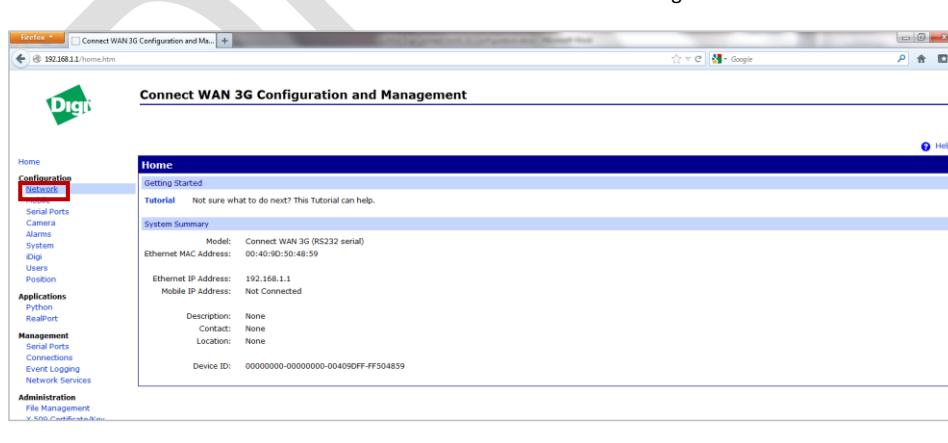
- From the “Digi Connect WAN 3G Configuration and Management, Apply Changes” screen click “Apply.”



- From the “Digi Connect WAN 3G Configuration and Management, Reconnect In Progress” screen and wait for the “Digi Connect WAN 3G Configuration and Management” home screen to appear. If you are not re-directed within a few minutes, click on the “click here” link.



- From the “Digi Connect WAN 3G Configuration and Management, Home” screen, click on the “Network” link on the left side of the screen under “Configuration.”



12. From the “Digi Connect WAN 3G Configuration and Management, Network Configuration” screen, click on the “DHCP Server Settings” menu link as shown below.

The screenshot shows the Digi Connect WAN 3G Configuration and Management interface. On the left, there's a navigation sidebar with sections like Home, Configuration, Applications, and Administration. The main area is titled 'Network Configuration' and contains a 'DHCP Server Settings' link, which is highlighted with a red box. Other links in this section include 'Ethernet IP Settings', 'Network Services Settings', 'Dynamic DNS Update Settings', 'IP Filtering Settings', and 'IP Forwarding Settings'. There are also 'Help' and 'Logout' buttons at the bottom right.

13. From the “Digi Connect WAN 3G Configuration and Management, DHCP Server Settings” screen, make the following changes:
- Change the “*IP Addresses” field to indicate: 192.168.1.2 to 192.168.1.10.
 - Check the box to the left of “Check that an IP address is not in use before offering it.”
 - Scroll down and click “Apply.”

This screenshot shows the 'DHCP Server Settings' configuration page. It includes fields for 'Scope Name' (set to 'eth0'), 'IP Addresses' (set to '192.168.1.2 to 192.168.1.10'), 'Lease Duration' (set to '1 days 0 hrs 0 mins'), and 'Delay' (set to '500 ms'). There are also checkboxes for 'Wait specified delay before sending DHCP offer reply' and 'Check that an IP address is not in use before offering it.' (which is checked). Below these, there's a section for 'Send a default gateway in the client lease (DHCP Option 3: Routers on Subnet)'. The 'IP address of scope interface (default)' radio button is selected. At the bottom, there's a table for 'Static Lease Reservations' with one entry: 'IP Address' 0.0.0 and 'MAC Address' 00:00:00:00:00:00. A 'Remove All' button is also present.

14. From the “Digi Connect WAN 3G Configuration and Management, Network Configuration” screen, scroll down and click on the “IP Forwarding Settings” menu link as shown below.

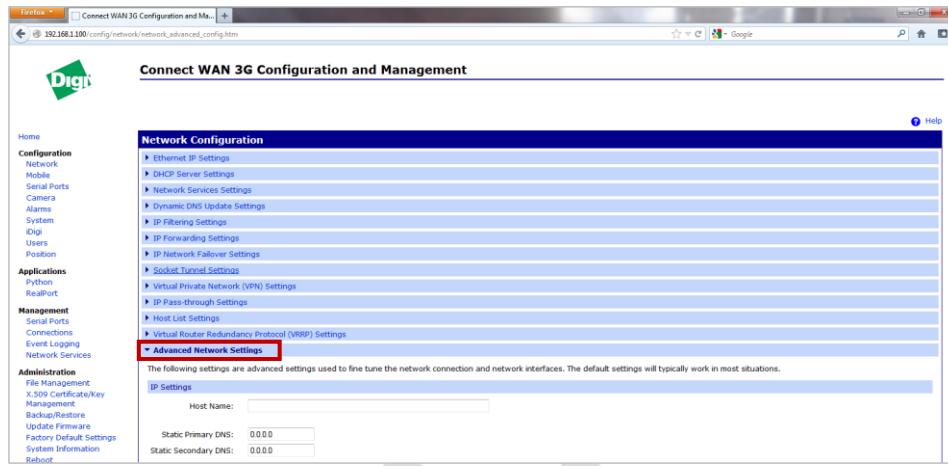
The screenshot shows the Digi Connect WAN 3G Configuration and Management interface. The left sidebar contains navigation links for Home, Configuration, Applications, Management, Administration, and Logout. The main content area is titled "Network Configuration" and includes sections for Ethernet IP Settings, DHCP Server Settings, Network Services Settings, Dynamic DNS Update Settings, IP Filtering Settings, and IP Forwarding Settings. The "IP Forwarding Settings" link is highlighted with a red box. Below it, there is a note about managing IP routing and a table for static routes. A note also states that if IP Routing is disabled, NAT is disabled. There is a section for Network Address Translation (NAT) settings with a table for NAT instances.

15. Under “Current Settings for NAT Instance 1,” scroll down to “Forward TCP/UDP/FTP connections from external networks to the following internal devices.” Change the forwarding rules for ports 22, 443, 2021, 8686 and 8080 to match the diagram below.

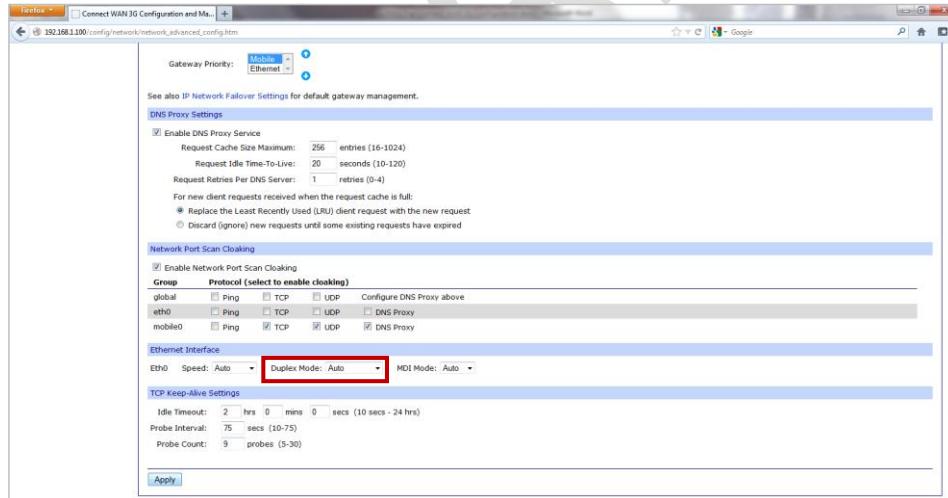
NOTE: On port 8080, the “Forward To Internal IP Address” and “Forward To Internal Port” settings differ from the first four ports.

The screenshot shows the "Current Settings for NAT Instance 1" section. It includes fields for enabling NAT and specifying the NAT Public Interface as "mobile0". There is also a checkbox for enabling DMZ Forwarding. Below this, there is a table for "Forward protocol connections from external networks to the following internal devices". The table has columns for Enable, Protocol, External Port, Forward To Internal IP Address, Forward To Internal Port, and Range Port Count. A specific row for port 8080 is highlighted with a red box, showing "192.168.1.11" in the "Forward To Internal IP Address" field and "80" in the "Forward To Internal Port" field. A note at the bottom states that port 8080 may require 64K to be forwarded (due to port range limit).

16. From the “Digi Connect WAN 3G Configuration and Management, Network Configuration” screen, scroll down and click on the “Advanced Network Settings” menu link.



17. Scroll down to “Ethernet Interface, Eth0” and change the “Duplex Mode” to “Auto” and then click on “Apply.”

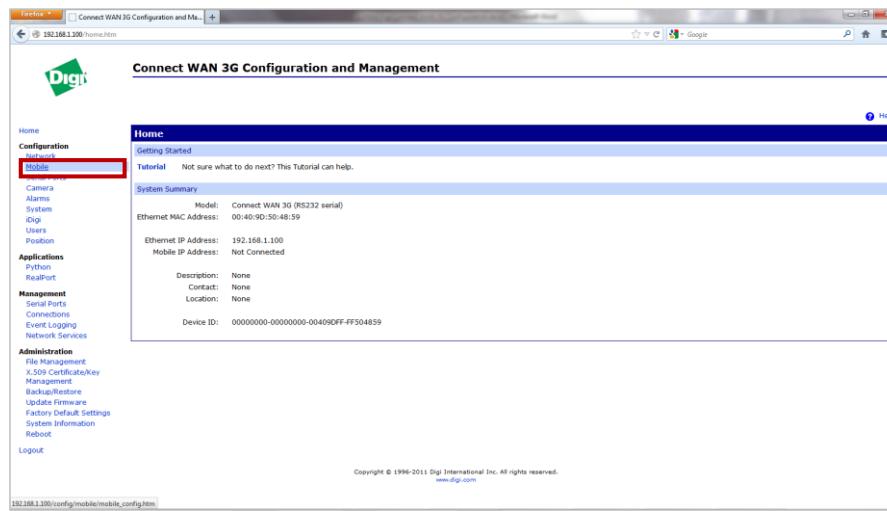


18. You have completed the basic network configuration for operation of your Digi WAN Connect 3G modem. The following two sections give provide basic mobile configuration setting that are dependent on your wireless carrier and their predominant wireless data technology.

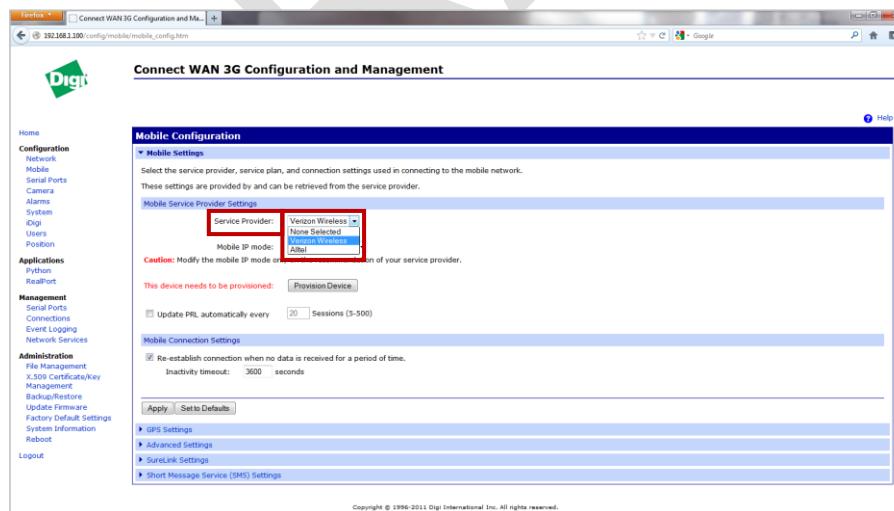
3.3 Mobile Configuration for a CDMA/1xRTT/EVDO Carrier

NOTE: Some steps may need to be added or skipped depending on your wireless carrier and their technology.

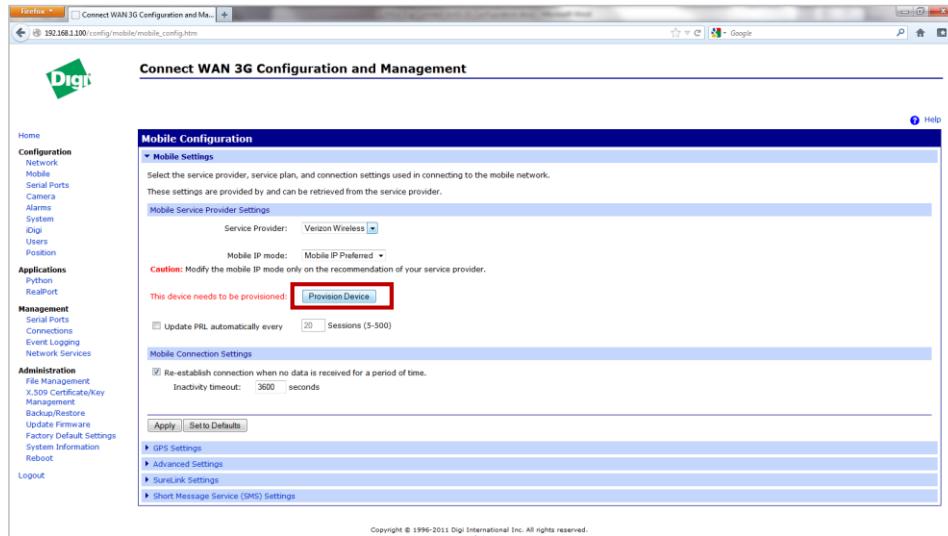
- From the “Digi Connect WAN 3G Configuration and Management, Home” screen, click on the “Mobile” link on the left side of the screen under “Configuration.”



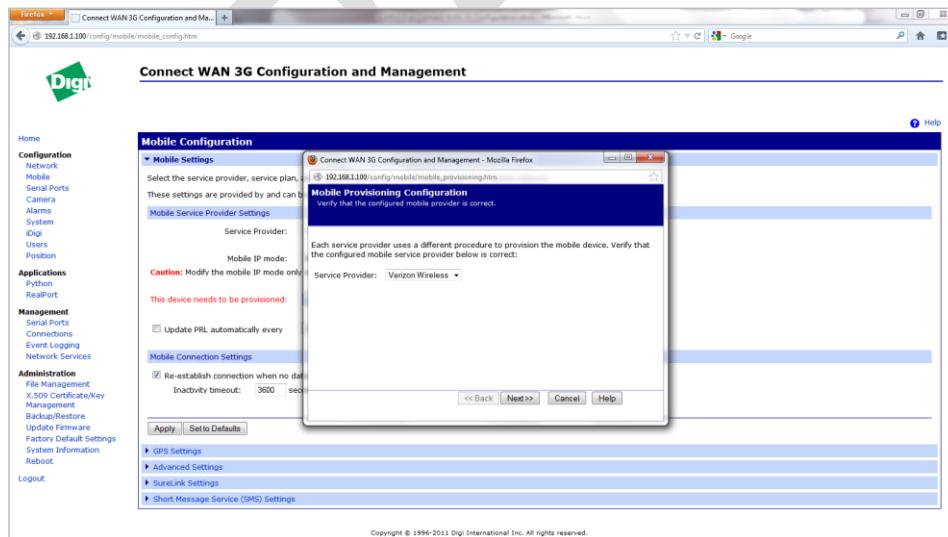
- From the “Digi Connect WAN 3G Configuration and Management, Mobile Configuration” screen, choose your wireless carrier from the “Service Provider” pull down menu.

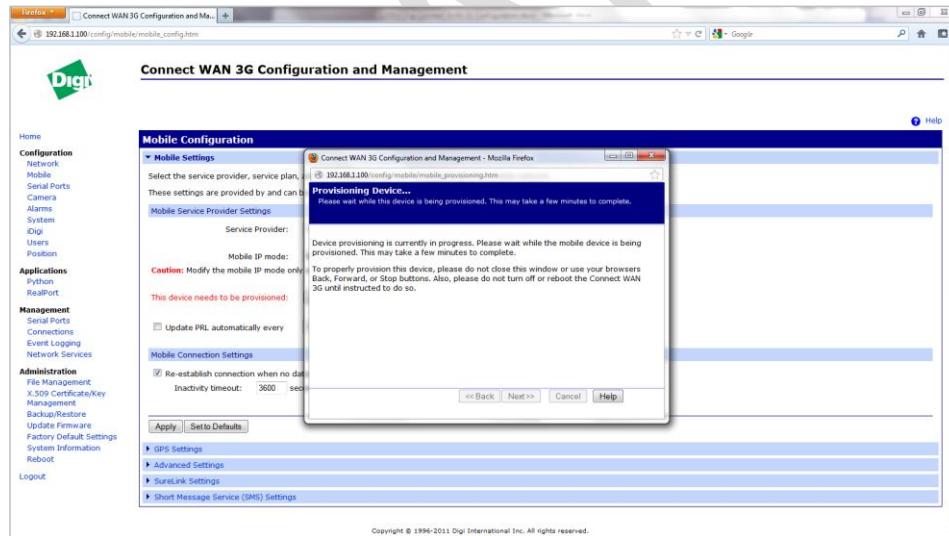
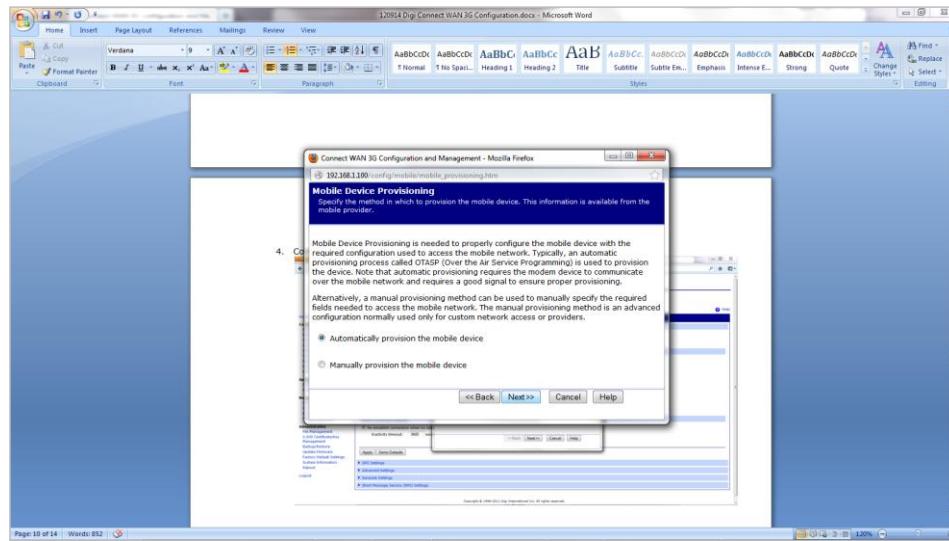


3. Click on “Provision Device.”

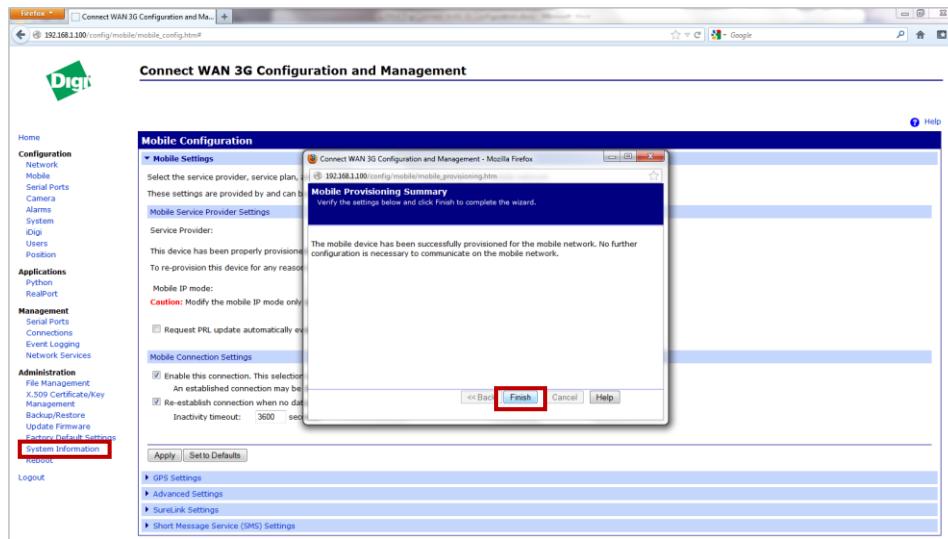


4. Confirm the settings on the “Mobile Provisioning Configuration” pop-up windows that follow. Click on the “Next” button to proceed to the next pop-up window.

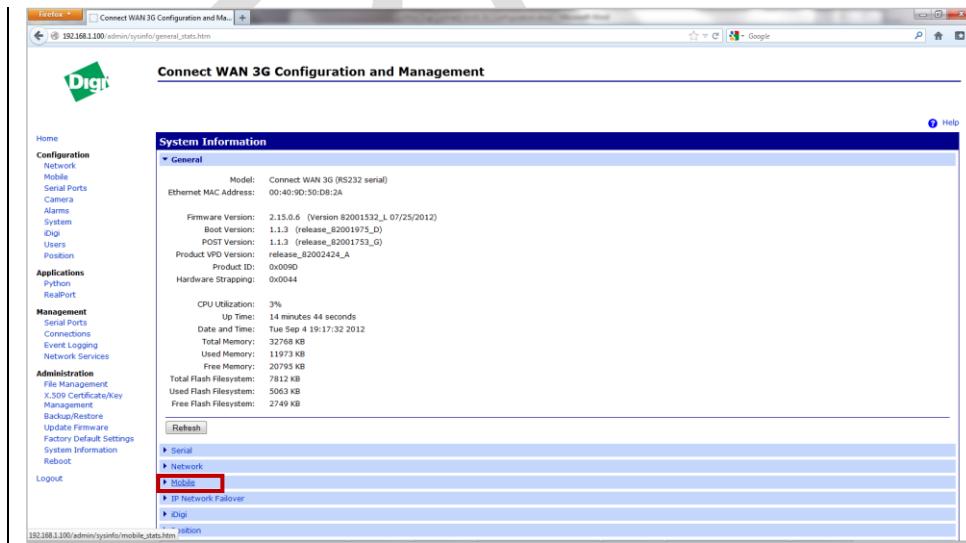




- When you receive the “Mobile Provisioning Summary” pop-up window indicating that your modem has been successfully provisioned, click on the “Finish” button. Then Click on the “System Information” link on the left hand Administration menu.



- Click on the “Mobile” link on the “Connect WAN 3G Configuration and Management, System Information” screen.



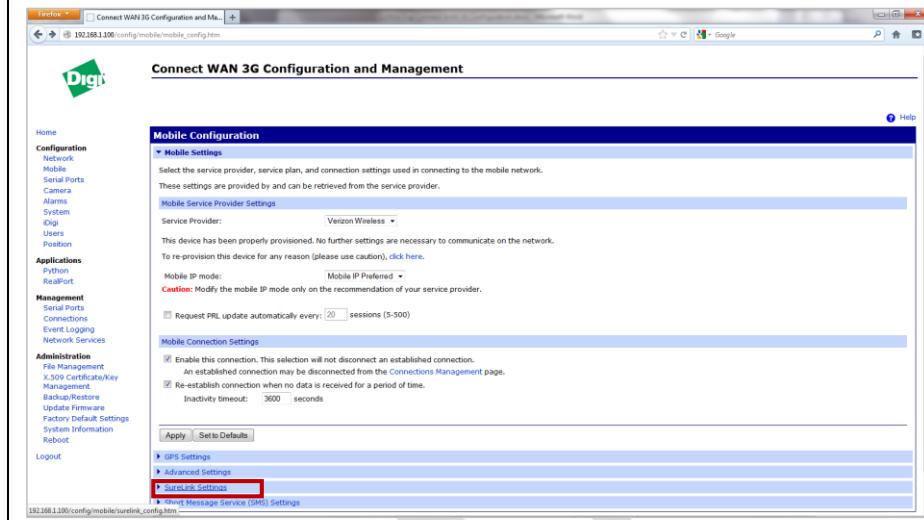
7. Verify that your mobile information is correct.

The screenshot shows a web-based management interface for a Digi device. The left sidebar contains navigation links for Home, Configuration (Network, Mobile, Serial Ports, Camera, Alarms, System, iDig, Users, Position), Applications (Python, RealPort), Management (Serial Ports, Connections, Event Logging, Network Services), Administration (File Management, X.509 Certificate/Key Management, Backup/Restore, Update Firmware, Factory Default Settings, System Information, Reboot, Logout). The main content area is titled 'System Information' and has a 'Mobile' section expanded. It displays mobile connection status, signal strength (1xRTT and EVDO), and mobile statistics including IP address, DNS addresses, data received/sent, and timer information.

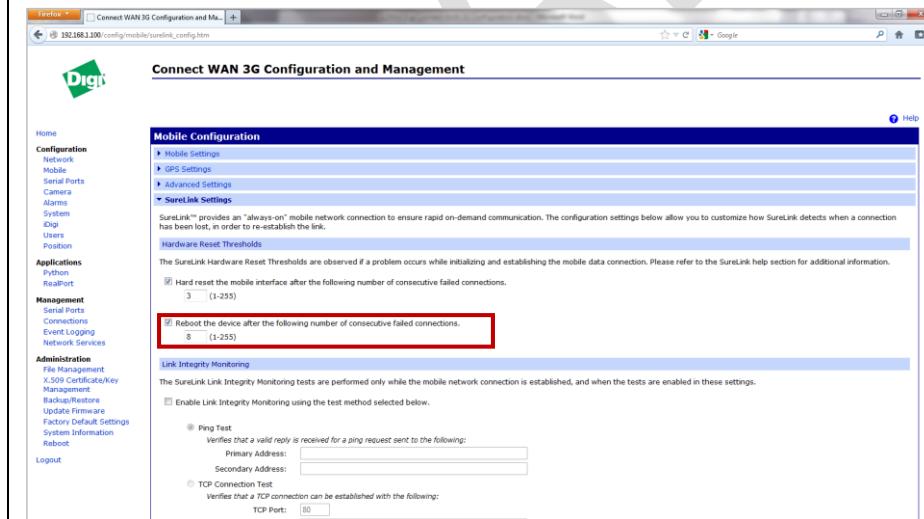
8. On the “Connect WAN 3G Configuration and Management, System Information” screen, click on the “Mobile” link on the left side of the screen under “Configuration.”

This screenshot is identical to the one above, but the 'Mobile' link in the 'Configuration' section of the sidebar is highlighted with a red box. This indicates the step where the user should click on the 'Mobile' link.

9. Scroll down on the screen and click on the “SureLink Settings” link on the bottom menu.



10. From the “SureLink Settings” screen, check the box for “Reboot the device after the following number of consecutive failed connections” and change the value to 8.



11. Scroll down and click on the “Apply” button.
12. Your backhaul modem is configured and ready for use.

NOTE: Users are strongly encouraged to follow the basic security settings that after completing the Mobile Configuration steps.

3.4 Mobile Configuration for a GSM/UMTS/HSPA Wireless Carriers

NOTE: Some steps may need to be added or skipped depending on your wireless carrier and their technology.

1. Before powering your Digi Connect WAN 3G GSM/UMTS/HSPA modem, remove the cover on the right side of the modem and insert your carrier's SIM card into SIM slot 1.
2. From the "Digi Connect WAN 3G Configuration and Management, Home" screen, click on the "Mobile" link on the left of the screen under "Configuration."

The screenshot shows the 'Mobile' configuration page. On the left, there is a navigation menu with 'Mobile' highlighted. The main area displays system summary information including Model: Connect WAN 3G (RS232 serial), Ethernet MAC Address: 00:40:90:50:48:59, Ethernet IP Address: 192.168.1.100, and Mobile IP Address: Not Connected. Below this, there are fields for Description, Contact, and Location, all set to 'None'. At the bottom, the Device ID is listed as 00000000-00000000-004090FF-FF504859.

3. From the "Digi Connect WAN 3G Configuration and Management, Mobile Configuration" screen, choose your wireless carrier from the "Service Provider" pull down menu.

The screenshot shows the 'Mobile Configuration' page. On the left, there is a navigation menu with 'Mobile' highlighted. The main area has a section for 'Mobile Service Provider Settings' where 'Service Provider: A&T/Cingular Wireless (Orange Network)' is selected. Below this, there are fields for 'Service Plan / APN: iGold', 'Username: (Optional)', and 'Password: (Optional)'. Under 'Mobile Connection Settings', there is a checkbox for 'Re-establish connection when no data is received for a period of time.' with an 'Inactivity timeout: 3600 seconds' setting. At the bottom, there are 'Apply' and 'Set to Defaults' buttons.

4. From the “Digi Connect WAN 3G Configuration and Management, Mobile Configuration” screen, enter your “Service Plan/APN” and click “Apply.”
5. Click on the “System Information” link on the left side of the screen under “Administration.”

Mobile Configuration

Select a SIM to configure from the list below.
Settings on this page apply to the selected SIM.

SIM:	Slot 1	<input checked="" type="button"/> Set as Primary
IMEI:	3101410427244688	
ICCID:	89014104254272446884	
Phone Number:	18538328465	
Status:	Primary	

Mobile Settings

Select the service provider, service plan, and connection settings used in connecting to the mobile network.
These settings are provided by and can be retrieved from the service provider.

Mobile Service Provider Settings

Service Provider:	AT&T/Cingular Wireless (Orange Network)
Service Plan / APN:	i2gold
Username:	(Optional)
Password:	(Optional)

Mobile Connection Settings

Re-establish connection when no data is received for a period of time.
Inactivity timeout: 3600 seconds

Apply | Set to Defaults

6. Click on the “Mobile” link located on the lower part of the “Connect WAN 3G Configuration and Management, System Information” screen.

System Information

General

Model:	Connect WAN 3G (RS232 serial)
Ethernet MAC Address:	00:40:9D:50:D8:2A
Firmware Version:	2.15.0.6 (Version 82001532_L_07/25/2012)
Boot Version:	1.1.3 (release_82001975_D)
POST Version:	1.1.3 (release_82001753_G)
Product VPD Version:	release_82002424_A
Product ID:	0x0090
Hardware Strapping:	0x0044

CPU Utilization:	3%
Up Time:	14 minutes 44 seconds
Date and Time:	Tue Sep 4 19:17:32 2012
Total Memory:	32768 KB
Used Memory:	11973 KB
Free Memory:	20795 KB

Total Flash Filesystem:	7812 KB
Used Flash Filesystem:	5063 KB
Free Flash Filesystem:	2749 KB

Refresh | Serial | Network | Mobile | IP Network Failover | Digi | System

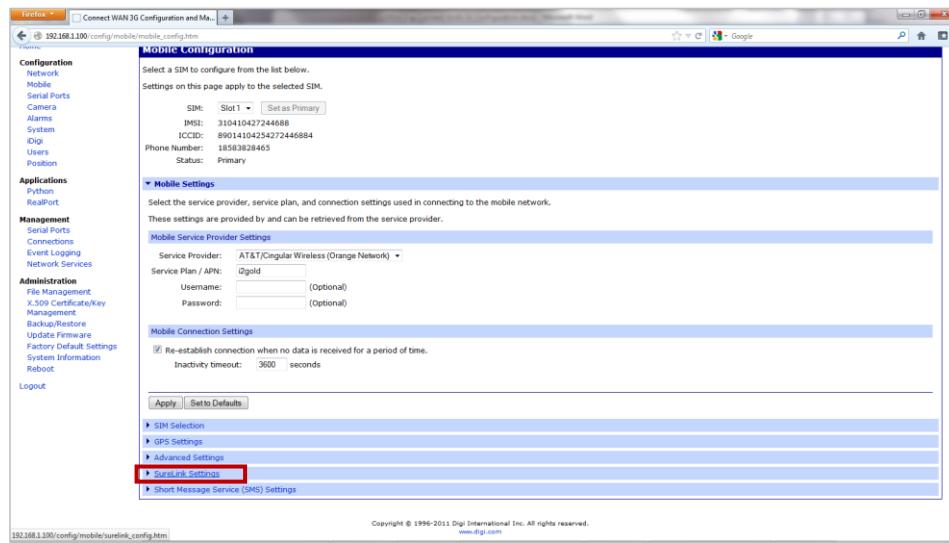
7. Verify that your mobile information is correct.

The screenshot shows the 'Connect WAN 3G Configuration and Management' interface. On the left, a navigation menu includes 'Mobile' under the 'Configuration' section. The main area displays 'System Information' with tabs for 'General', 'Serial', 'Network', and 'Mobile'. The 'Mobile' tab is selected, showing details for SIM cards and mobile connections. A table lists SIM cards with columns for Slot, IMEI and ICCID, Phone Number, Status, PIN Status, and Active. It shows two entries: Slot 1 with IMEI 310410427244688 and Slot 2 with IMEI N/A. Below this is a 'Mobile Connection' section with registration status, location area code (0x7C14), cell ID (0x023296B1), and signal strength (-69 dBm). At the bottom is a 'Mobile Statistics' section with IP address (166.130.46.233), primary DNS (209.183.33.23), secondary DNS (0.0.0.0), data received (322 bytes), and data sent (92 bytes).

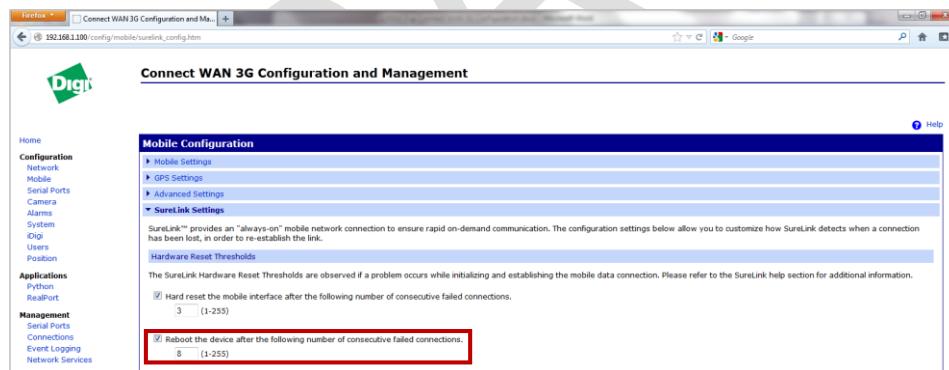
8. On the "Connect WAN 3G Configuration and Management, System Information" screen, click on the "Mobile" link on the left side of under "Configuration."

This screenshot is identical to the one above, showing the 'Connect WAN 3G Configuration and Management' interface. However, the 'Mobile' link in the navigation menu on the left is highlighted with a red box, indicating it has been selected. The rest of the interface and its content are the same as the first screenshot.

9. Scroll down and click on the “SureLink Settings” link located near the bottom of the screen.



10. From the “SureLink Settings” screen, check the box for “Reboot the device after the following number of consecutive failed connections” and change the value to 8.



11. Scroll down and click on the “Apply” button. Your backhaul modem is configured and ready for use.

NOTE: Users are strongly encouraged to follow the basic security settings that follow the Mobile Configuration steps.

3.5 Basic Security Settings

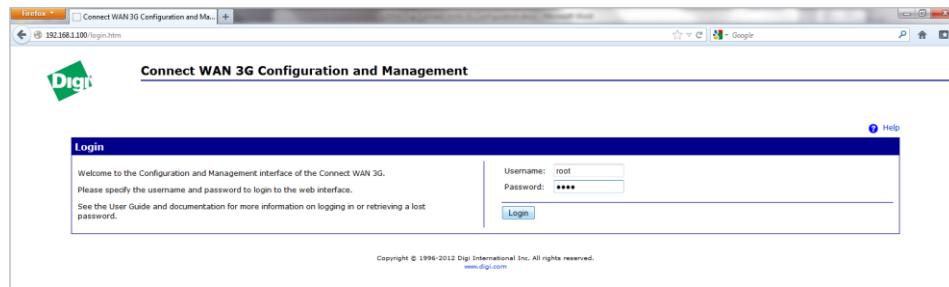
- From the “Digi Connect WAN 3G Configuration and Management, Home” screen, click on the “Users” link on the left side of the screen under “Configuration.”

The screenshot shows the 'Connect WAN 3G Configuration and Management' interface. On the left, a sidebar menu includes 'Home', 'Configuration' (with 'Users' highlighted), 'Network', 'Mobile', 'Serial Ports', 'Camera', 'Alarms', 'System', 'Logs', 'Applications', 'Python', 'RealPort', 'Management', 'Serial Ports', 'Connections', 'Event Logging', 'Network Services', and 'Administration'. The main content area displays 'System Summary' with device information: Model: Connect WAN 3G (RS232 serial), Ethernet MAC Address: 00:40:90:50:D8:2A, Ethernet IP Address: 192.168.1.100, Mobile IP Address: 166.140.215.184, Description: None, Contact: None, Location: None, and Device ID: 00000000-00000000-004090FF-FF50082A.

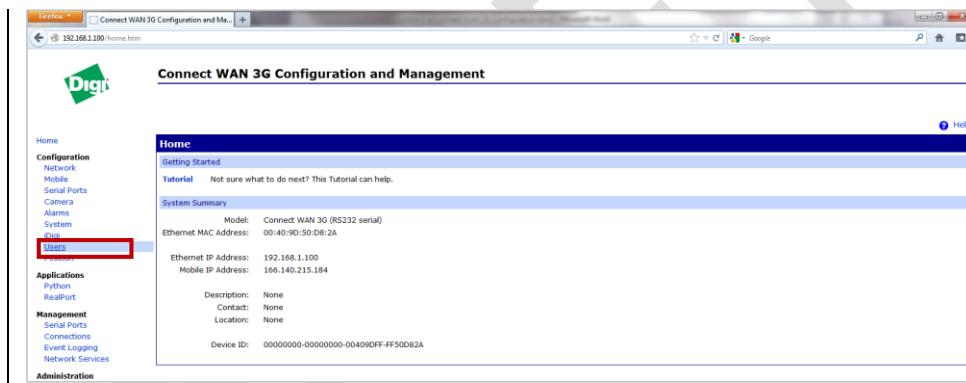
- From the “Digi Connect WAN 3G Configuration and Management, Users Configuration” screen, check the box for “Enable user logins” and click the “Apply” button.

The screenshot shows the 'Users Configuration' screen. The sidebar is identical to the previous one. The main content area has a note: "After enabling user logins, you will immediately be asked to log in to the web interface. Be certain that you know a valid user name and password combination that you previously configured, or the device default values if you have never configured users and passwords. If you do not know a valid combination, you will not be able to log into this device after you enable user logins." Below this, there is a checkbox labeled "Enable user logins" which is checked and highlighted with a red box. There is also an "Apply" button. The 'Available Users' section shows a table with one row: User Name: root.

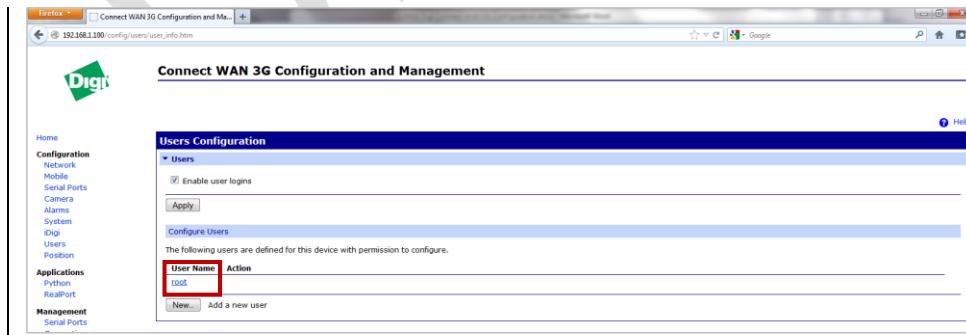
3. On the “Digi Connect WAN 3G Configuration and Management” Login screen, log in with username: root and default password: dbps.



4. From the “Digi Connect WAN 3G Configuration and Management, Home” screen, click on the “Users” link on the left side of the screen under “Configuration.”



5. From the “Digi Connect WAN 3G Configuration and Management, User Configuration” screen, click on the “root” User Name link.



6. From the “Digi Connect WAN 3G Configuration and Management, User Configuration – root” screen, do the following:
 - Click change and confirm that the “root” password meets or exceeds your company’s requirements.
 - Click on the “Apply” button.

The screenshot shows a Firefox browser window with the URL 192.168.1.100/config/users/user_config_edit.html. The page title is "Connect WAN 3G Configuration and Management". On the left, there's a navigation menu with items like Home, Configuration, Network, Mobile, Serial Ports, Camera, Alarms, System, Digi, I/O, Users, Position, Application, Python, and RealPort. The main content area is titled "User Configuration - root" and contains a "User Configuration" section with fields for User Name (root), New Password (****), and Confirm Password (****). There's also an "Apply" button and links for User Access and User Permissions. A "Help" link and a "Return to Users..." link are at the top right.

7. For additional security settings, contact you On-Ramp Wireless representative with root access information so that we may configure IP filtering and additional security settings appropriate for your configuration.
8. Refer to Chapter 4: Connecting the AP to the RPMA Network.

3.6 Port Forwarding Configuration Process

1. Certain incoming TCP/IP ports that come in over the PPP link/WWAN must be Port Forwarded to the AP at **192.168.1.1**. All other incoming ports should remain blocked unless they are required for other applications. These ports are:
 - 22 TCP ssh
 - 1161 TCP snmp
 - 443 TCP https
 - Any other port(s) required to maintain the backhaul modem or other equipment at the customers site remotely

The screenshot shows the "IP Routing and Static Route Settings" section. It includes a note about managing IP routing (forwarding) between network interfaces and using static routes. It has sections for "IP Routing and Static Route Settings" and "IP Forwarding Settings". Under "IP Forwarding Settings", there's a table for adding static routes. The table has columns: Enable, Destination Network, Netmask, Gateway Address, Metric, and Interface. A note says "No static routes have been added". An "Add" button is present. A yellow callout box labeled "Formatted: Font: Calibri" points to the "Font" setting in the table header.

Network Address Translation (NAT) Settings

Select from these Network Address Translation (NAT) instances:

Instance	Enabled	Interface Name	Action
Instance 1	yes	mobile0	(Displayed) Set to Defaults
Instance 2	no	None Selected	View / Edit Set to Defaults
Instance 3	no	None Selected	View / Edit Set to Defaults
Instance 4	no	None Selected	View / Edit Set to Defaults
Instance 5	no	None Selected	View / Edit Set to Defaults
Instance 6	no	None Selected	View / Edit Set to Defaults

Current Settings for NAT Instance 1:

Enable Network Address Translation (NAT)
 NAT Public Interface: mobile0
 NAT Table Size Maximum: 256 entries (64-1024)
 Enable Loose Outbound IP Fragment Translation/Forwarding
 Enable DMZ Forwarding to this IP address: 0.0.0.0

Forward protocol connections from external networks to the following internal devices:

Enable	Forward This Protocol	Forward To Internal IP Address
<input type="checkbox"/>	GRE	0.0.0.0
<input type="checkbox"/>	ESP	0.0.0.0

Forward TCP/UDP/FTP connections from external networks to the following internal devices (you may configure up to 64 forwarding rules):

Enable	Protocol	External Port	Forward To Internal IP Address	Forward To Internal Port	Range Port Count
<input checked="" type="checkbox"/>	TCP	22	192.168.1.1	22	1 Remove
<input checked="" type="checkbox"/>	TCP	443	192.168.1.1	443	1 Remove
<input checked="" type="checkbox"/>	TCP	8686	192.168.1.1	8686	1 Remove
<input checked="" type="checkbox"/>	TCP	1161	192.168.1.1	1161	1 Remove
<input checked="" type="checkbox"/>	TCP	161	192.168.1.11	161	1 Remove
<input checked="" type="checkbox"/>	TCP				Add

Formatted: Font: Calibri

3.7 Customer-Owned Modem Backhaul Requirements

This section provides a basic list of requirements for modem configuration if using a modem that is not provided by On-Ramp Wireless. For any further questions regarding modem configuration, contact On-Ramp Wireless at support@onrampwireless.com.

1. The AP's default IP address is **192.168.1.1**. The AP's netmask is **255.255.255.0** and the default router is **192.168.1.254**. The Ethernet port on the modem should be set to **192.168.1.254**.
2. Certain incoming TCP/IP ports that come in over the PPP link/WWAN need to be Port Forwarded to the AP at **192.168.1.1**. All other incoming ports should remain blocked unless they are needed for other applications. These ports are:
 - 22 TCP ssh
 - 1161 TCP snmp
 - 443 TCP https
 - Any other port(s) required to maintain the backhaul modem or other equipment at the customers site remotely
3. If the backhaul modem has a stateful firewall the following subnets and IP addresses need to be allowed in IP filtering to reach the AP on **192.168.1.1**:
 - 206.190.87.192/27 255.255.255.224 On-Ramp Wireless Support
 - 69.43.176.160/27 255.255.255.224 On-Ramp Wireless Data Center (hosting)
 - Your company's IP subnets for your internal support/maintenance center should be opened also.

4. If the backhaul modem has a stateless firewall, the following IP addresses need to be allowed in IP filtering **in addition to** the addresses listed above:
 - [208.67.222.222 Open DNS](#)
 - [208.67.220.220 Open DNS](#)
 - [8.8.8.8 Google DNS](#)
 - [8.8.4.4 Google DNS](#)
 - [24.56.178.140 www.nist.gov NTP](#)
 - [164.67.62.194 tick.ucla.edu NTP](#)
 - [69.43.176.168 time.onrampwireless.com NTP](#)
5. On stateless and some stateful firewalls, outbound traffic is sometimes filtered. Our access point uses **TCP Port 5051** for communication to the gateway and **TCP Port 162** for **SNMP traps** to the EMS. These ports should be allowed to the same **subnets allowed in IP Filtering**.
6. All other IP addresses and ports that are not required for the AP operation or other applications at the customer's site should be blocked.
7. Add a secure username and password for On-Ramp Wireless support to use during troubleshooting and configuration.

3.8 Installation and Validation Process

When the modem is configured and validated, it is ready to be installed with the AP at the remote site. For specific physical installation instructions, refer to the [AP Deployment Guide \(010-0021-00\)](#).

4 Connecting the AP to the RPMA Network

The final step for connecting the AP to the RPMA network is registering the backhaul services with the AP via the EMS. To do this:

1. The RPMA Network Operator must interact with both the AP webpage and the EMS webpage.
2. The AP Network Installation Operator must submit a request to the RPMA Network Operator in order to complete the process for registering the AP.
3. If the RPMA network resides within the On-Ramp Wireless Hosted Environment, the AP Network Installation Operator must submit a request to support@onrampwireless.com to register the AP.
4. After completing this section, the AP is ready to accept over-the-air traffic from enabled and authorized endpoints. This process should be run by the RPMA Network Operator who can refer to the *EMS Operator Guide (010-0107-00)* for further details.

Prerequisites:

- RPMA Network Operator must have access to the AP webpage from the RPMA network.
- Important! In order for the AP to be fully tested when being added to the RPMA network, it should be located in a staging environment that includes installed and functional GPS and RF antennas. If the GPS antenna does not receive legitimate signal strength, then the AP will not be able to fully register to the RPMA network.
- The following checklist must be completed and submitted to the RPMA Network Operator after the AP is ready for RPMA Network registration. If the AP Installation Network Operator is the same individual as the RPMA Network Operator, then please refer to the EMS Operator Guide for instructions on how to register the Access Point to the RPMA network. If the AP is to be added to the On-Ramp Wireless Hosted Network, then the AP Installation Network Operator must submit the checklist to support@onrampwireless.com.

<u>AP Registration Prerequisite Checklist</u>	<u>All of the following fields MUST be completed before requesting the RPMA Network Operator to register the AP.</u>
<u>Static IP address of Access Point from the perspective of the RPMA Network Operator</u>	
<u>Is the AP in a staging environment or in a final deployment location?</u>	
<u>URL of how to access the AP web page</u>	
<u>The RF Cable Type and Length</u>	
<u>RF Antenna Height</u>	
<u>AP Site Name</u>	
<u>AP must be energized with the appropriate GPS Cable and RF antenna installed</u>	