Backhaul Selection and Configuration Manual

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

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.

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.

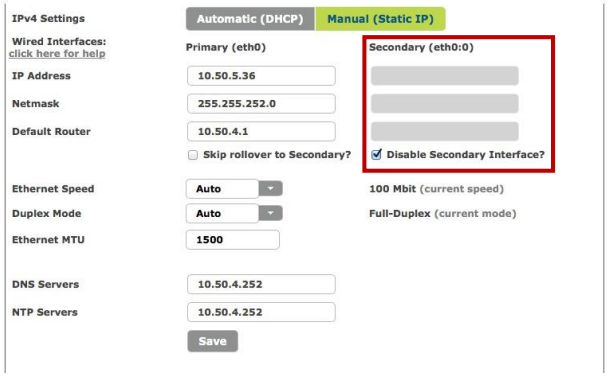
3. Enter the information obtained in section 2.1, into the fields indicated below.
   a. The static IP address in the ***IP Address*** field
   b. The Subnet Mask in the ***Netmask*** field
   c. The default route IP address in the ***Default Router*** field
   d. The DNS server(s) in the ***DNS Servers*** field
   e. The NTP server(s) in the ***NTP Servers*** field

~~3.~~4. Select ***Save*** button.

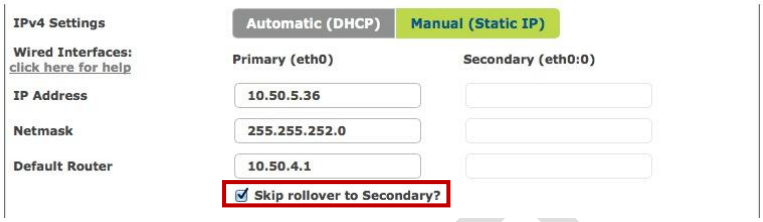
~~4.~~5. Select ***Reboot Access Point*** button.

~~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).



~~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.



~~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:

a. The NTP server is not configured correctly on the AP website.

b. The network routing rules between the AP and the NTP server are blocking connectivity.

c. 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)

~~12.~~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.
   - Sprint (CDMA) - U.S.
   - Verizon Wireless (CDMA) U.S., Puerto Rico
   - Rogers Wireless (GSM) - Canada
   - Midwest Wireless (CDMA) - U.S.
   - Alltel Wireless (CDMA) - U.S.
   - T-Mobile (GSM) - U.S.
   - Cellular One (GSM) - U.S.
   - Centennial Wireless (CDMA) - Puerto Rico
   - Claro PR (GSM) - Puerto Rico
   - IUSACELL (CDMA) - Mexico
   - Entel PCS (GSM) - Chile
   - Claro (GSM) - Peru
   - Vodaphone (GSM) – New Zealand
   - Comcel (GSM) - Colombia
   - IDA (GSM) - Singapore
   - Telstra (GSM) - Australia
   - Telefonica Moviles (GSM) - Guatemala, El Salvador
   - ICASA (GSM) - South Africa
   - Movistar - Panama (CDMA), Chile (GSM)
   - Anatel (GSM) - Brazil
   - Bell Mobility (CDMA) – Canada
   - Dalacom (CDMA) – Kazakhstan

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

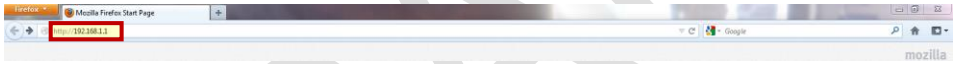
NOTE: Selection and use of an unsupported modem may limit AP performance, and could affect your ORW product warranty. Contact ORW to discuss BEFORE using a unsupported modem.

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

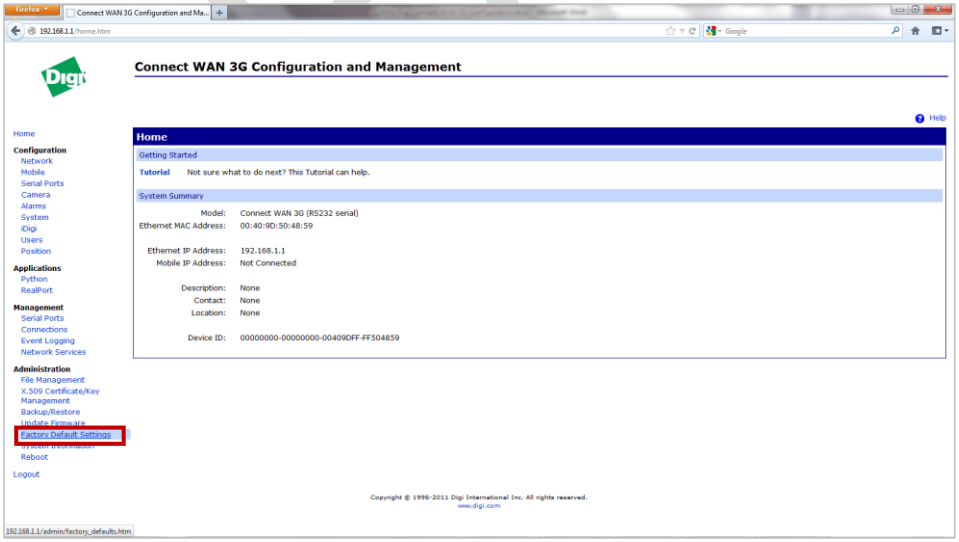
3.2 Basic Network Configuration

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.

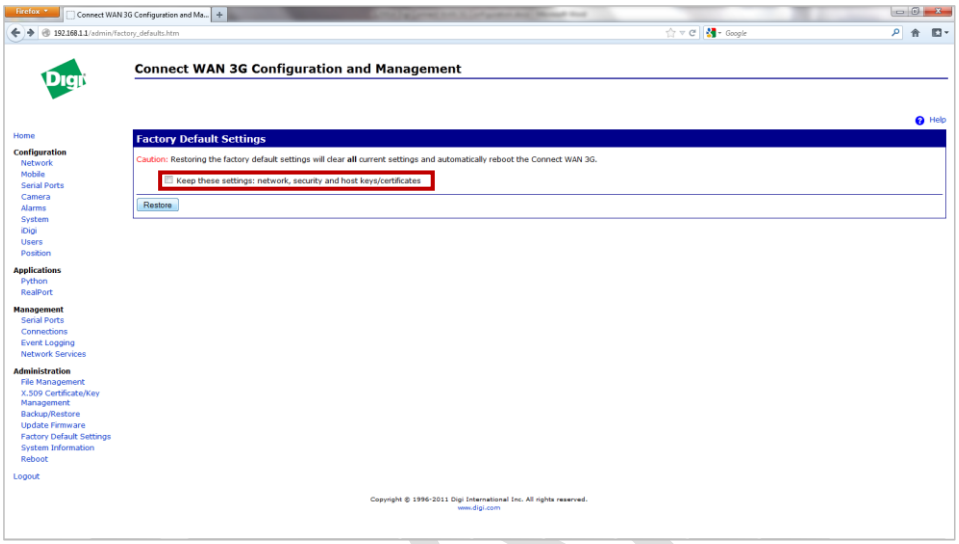
1. Configure your PC's wired Ethernet connection to:
   a. IP Address: 192.168.1.254
   b. Subnet Mask: 255.255.255.0
2. Open your web browser (IE, Chrome or Firefox).
3. In the URL location type http://192.168.1.1.



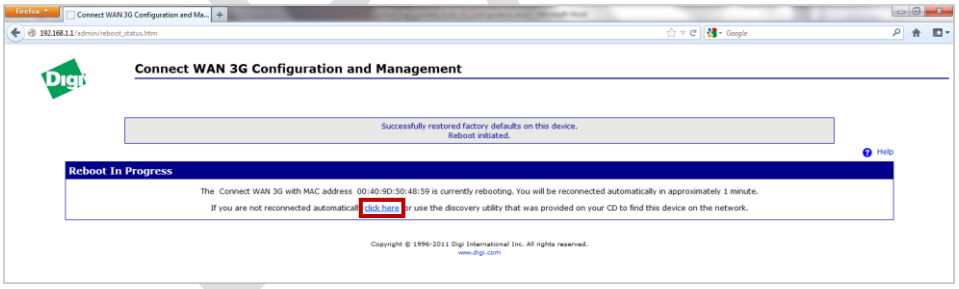
4. From the "Digi Connect WAN 3G Configuration and Management" home screen, click on the "Factory Default Settings" link on the left side of the screen under "Administration."



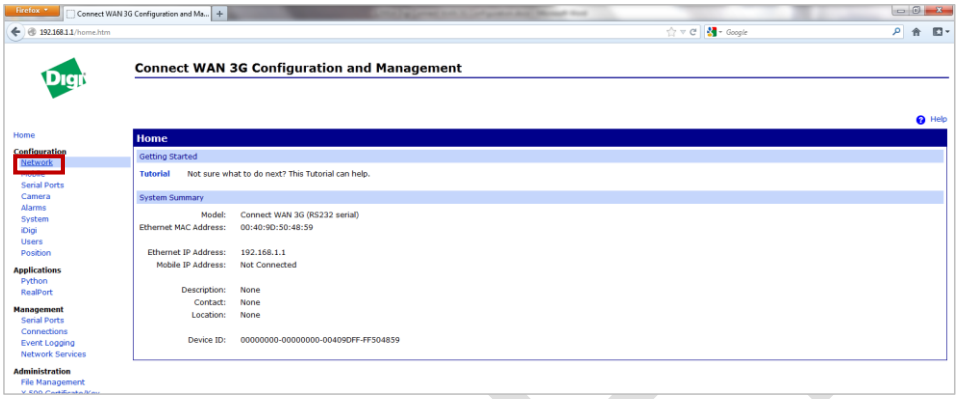
5. Uncheck the box for "Keep these settings: network, security and host keys/certificates" and click on the "Restore" Button.



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.”

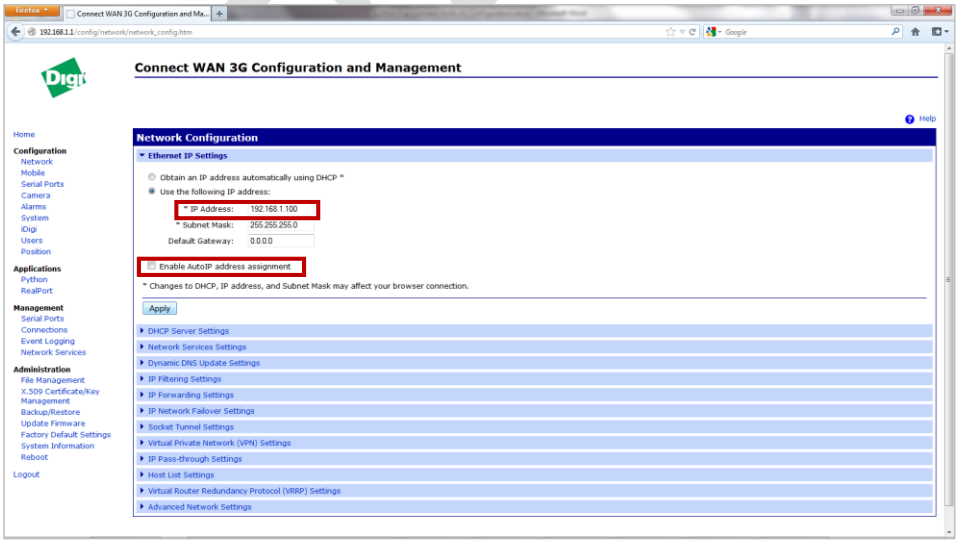


8. From the “Digi Connect WAN 3G Configuration and Management, Network Configuration” screen, changes:

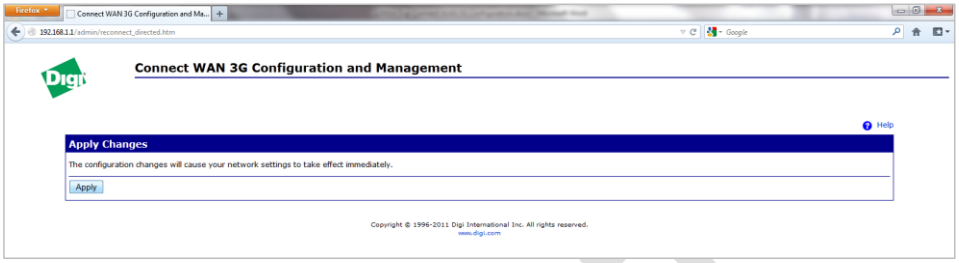
   a. Change the IP Address to 192.168.1.100.

   b. Un-check the “Enable Auto-IP address assignment” box.

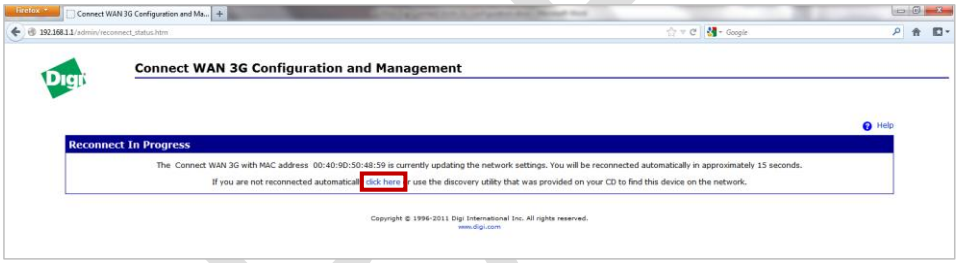
   c. Click “Apply.”



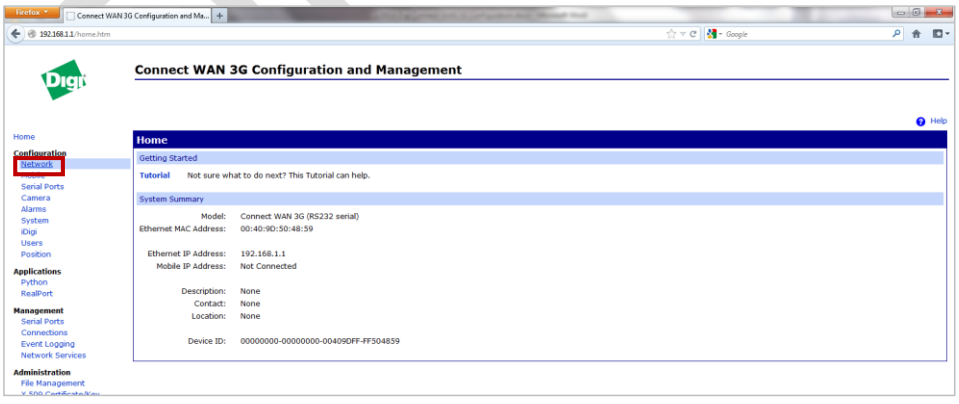
9. From the “Digi Connect WAN 3G Configuration and Management, Apply Changes” screen click “Apply.”



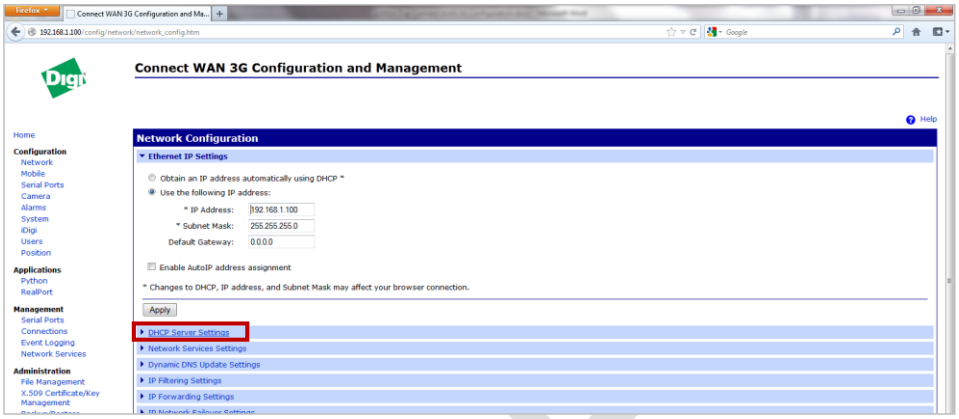
10. From the “Digi Connect WAN 3G Configuration and Management, Reconnect In Progress” screen and wait for the “Digi Connect WAN 3G Configuration and Management” home screen to appear. If you are not re-directed within a few minutes, click on the “click here” link.



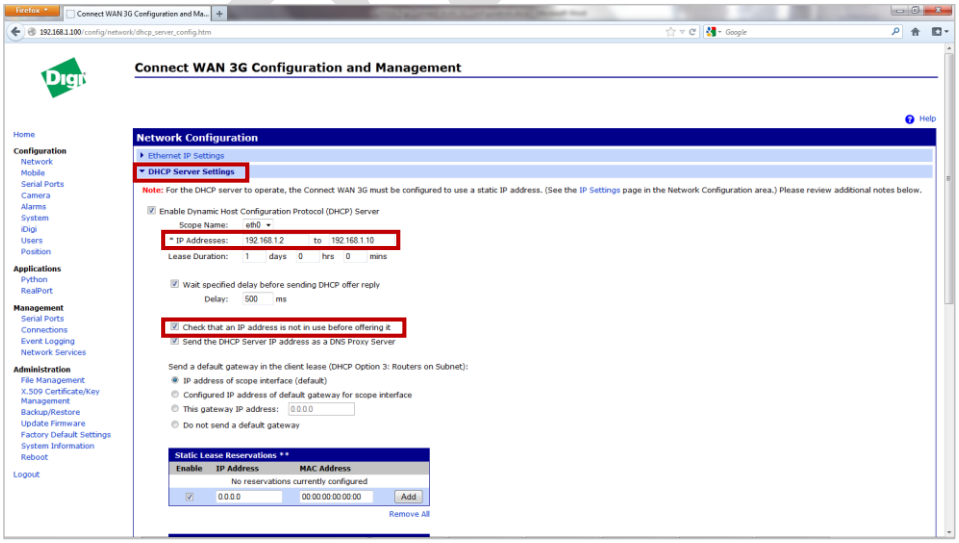
11. From the “Digi Connect WAN 3G Configuration and Management, Home” screen, click on the “Network” link on the left side of the screen under “Configuration.”



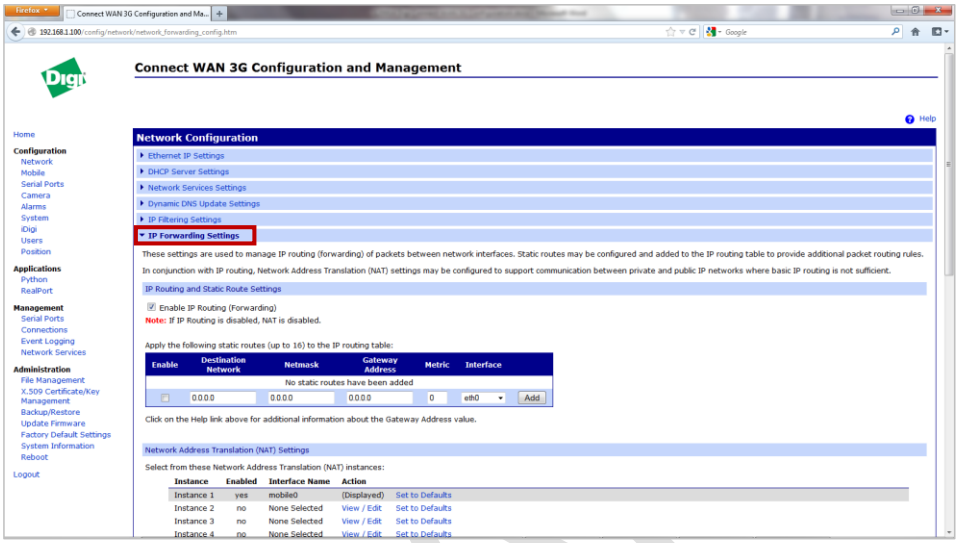
12. From the “Digi Connect WAN 3G Configuration and Management, Network Configuration” screen, click on the “DHCP Server Settings” menu link as shown below.



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

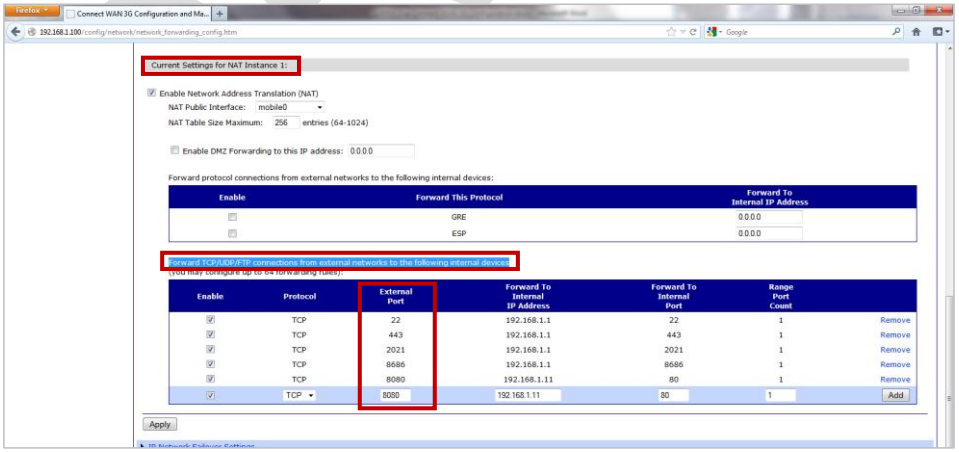


14. From the "Digi Connect WAN 3G Configuration and Management, Network Configuration" screen, scroll down and click on the "IP Forwarding Settings" menu link as shown below.

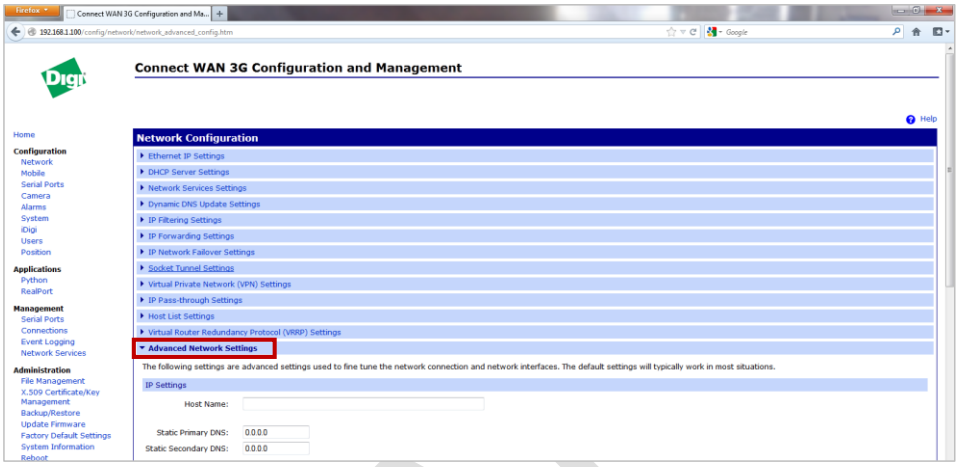


15. Under "Current Settings for NAT Instance 1," scroll down to "**Forward TCP/UDP/FTP connections from external networks to the following internal devices."** Change the forwarding rules for ports 22, 443, 2021, 8686 and 8080 to match the diagram below.

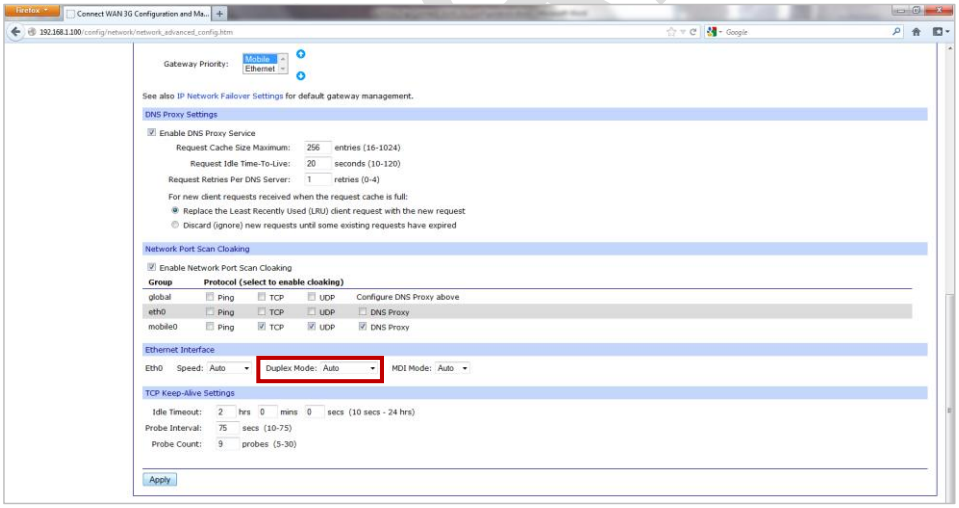
NOTE: On port 8080, the "Forward To Internal IP Address" and "Forward To Internal Port" settings differ from the first four ports.



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.”

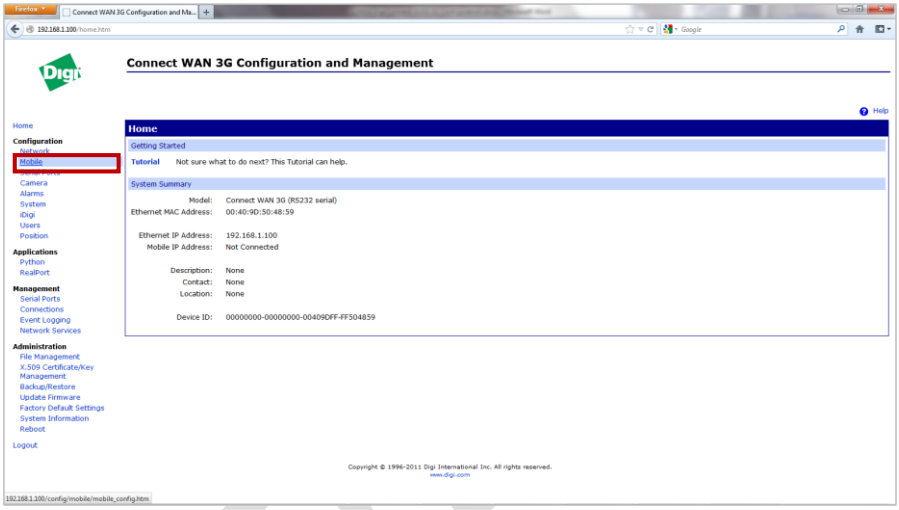


18. You have completed the basic network configuration for operation of your Digi WAN Connect 3G modem. The following two sections give provide basic mobile configuration setting that are dependent on your wireless carrier and their predominant wireless data technology.

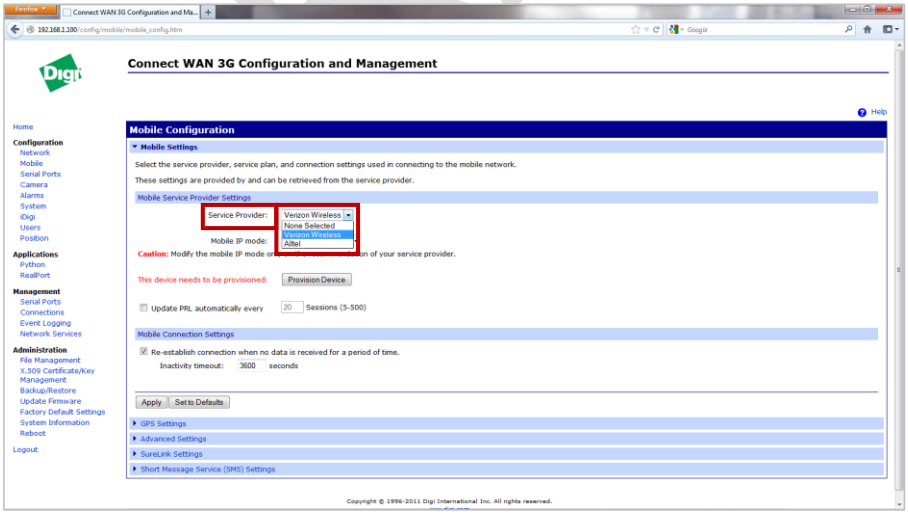
3.3 Mobile Configuration for a CDMA/1xRTT/EVDO Carrier

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

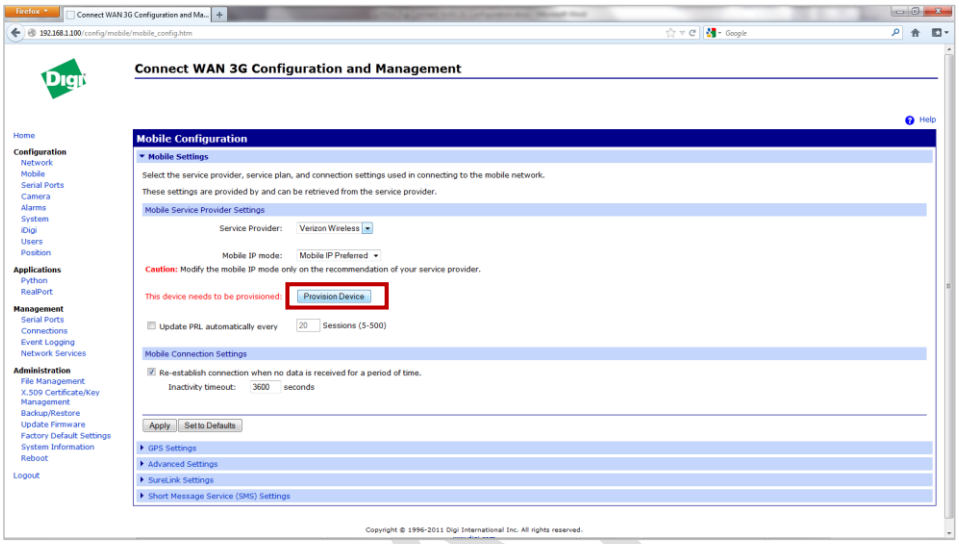
1. From the "Digi Connect WAN 3G Configuration and Management, Home" screen, click on the "Mobile" link on the left side of the screen under "Configuration."



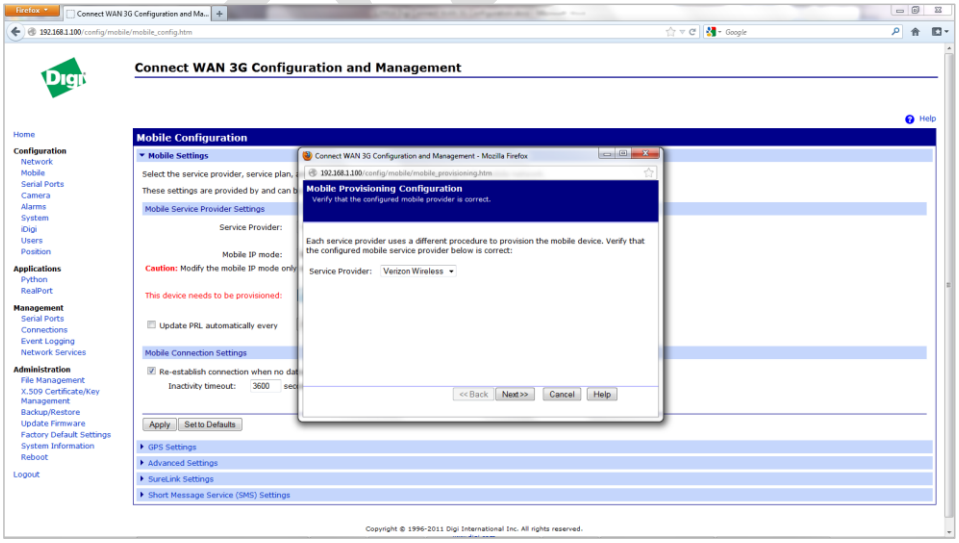
2. From the "Digi Connect WAN 3G Configuration and Management, Mobile Configuration" screen, choose your wireless carrier from the "Service Provider" pull down menu.

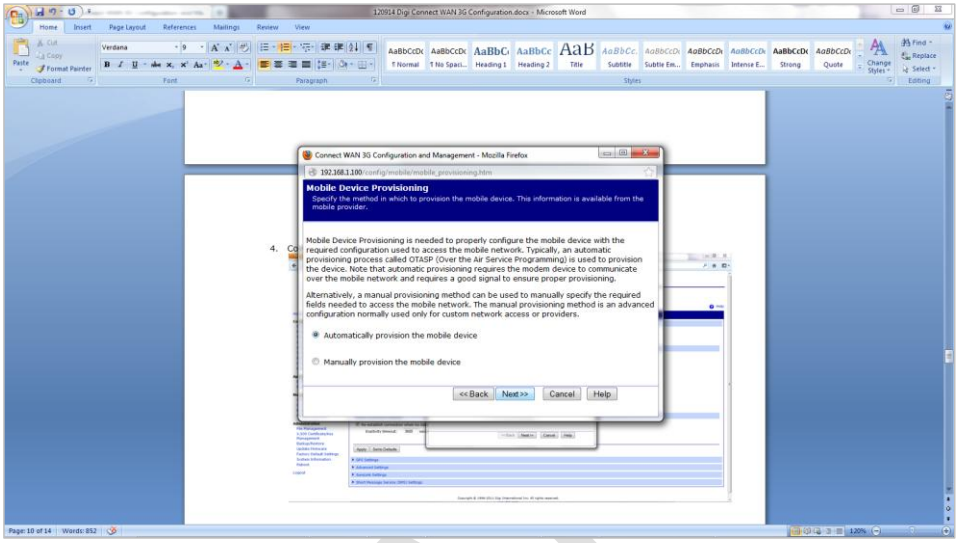


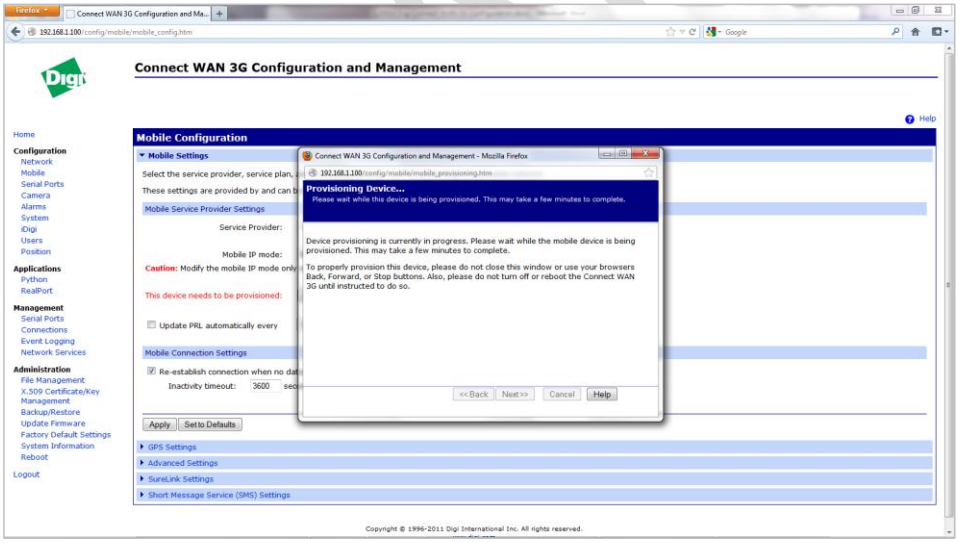
3. Click on “Provision Device.”



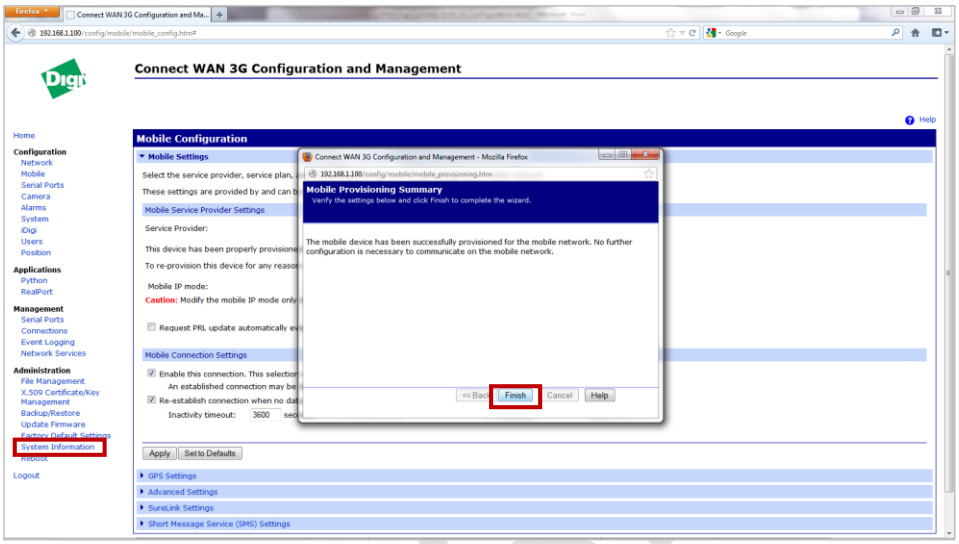
4. Confirm the settings on the “Mobile Provisioning Configuration” pop-up windows that follow. Click on the “Next” button to proceed to the next pop-up window.



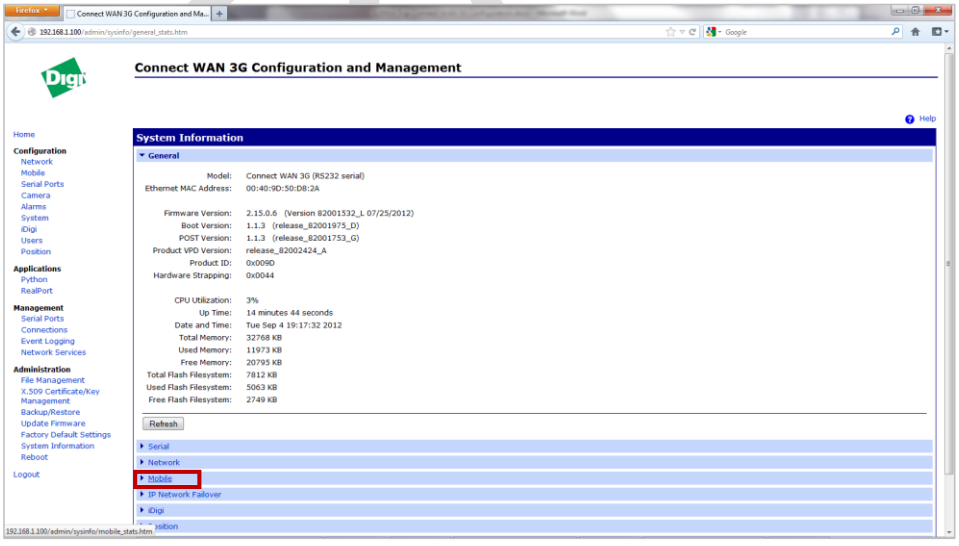

Connect WAN 3G Configuration and Management - Mozilla Firefox
Mobile Device Provisioning
Specify the method in which to provision the mobile device. This information is available from the mobile provider.
Mobile Device Provisioning is needed to properly configure the mobile device with the required configuration used to access the mobile network. Typically, an automatic provisioning process called OTASP (Over the Air Service Programming) is used to provision the device. Note that automatic provisioning requires the modem device to communicate over the mobile network and requires a good signal to ensure proper provisioning.
Alternatively, a manual provisioning method can be used to manually specify the required fields needed to access the mobile network. The manual provisioning method is an advanced configuration normally used only for custom network access or providers.
Automatically provision the mobile device
Manually provision the mobile device
<<Back
Next>>
Cancel
Help


Connect WAN 3G Configuration and Management
Mobile Configuration
Provisioning Device...
Please wait while this device is being provisioned. This may take a few minutes to complete.
Device provisioning is currently in progress. Please wait while the mobile device is being provisioned. This may take a few minutes to complete.
To properly provision this device, please do not close this window or use your browsers Back, Forward, or Stop buttons. Also, please do not turn off or reboot the Connect WAN 3G until instructed to do so.
Apply
Set to Defaults
Copyright © 1996-2011 Digi International Inc. All rights reserved.

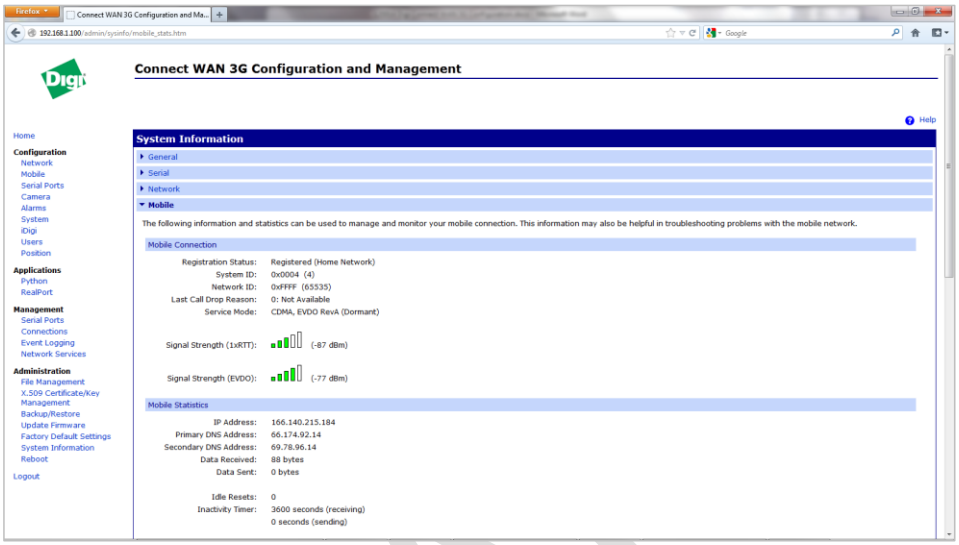
5. When you receive the “Mobile Provisioning Summary” pop-up window indicating that your modem has been successfully provisioned, click on the “Finish” button. Then Click on the “System Information” link on the left hand Administration menu.



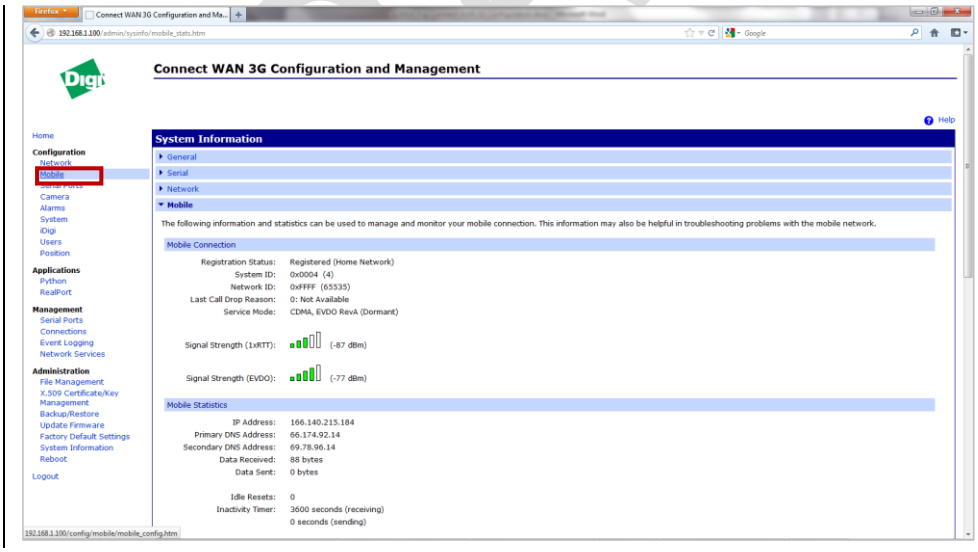
6. Click on the “Mobile” link on the “Connect WAN 3G Configuration and Management, System Information” screen.



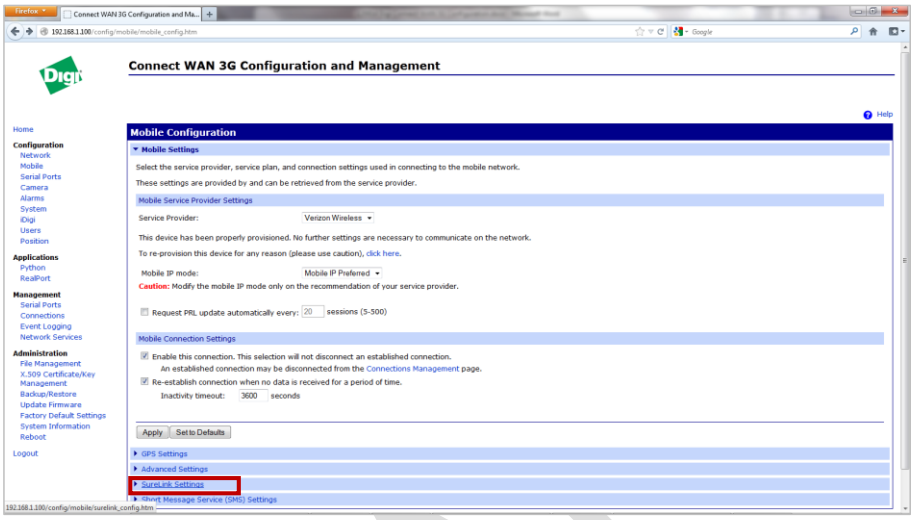
7. Verify that your mobile information is correct.



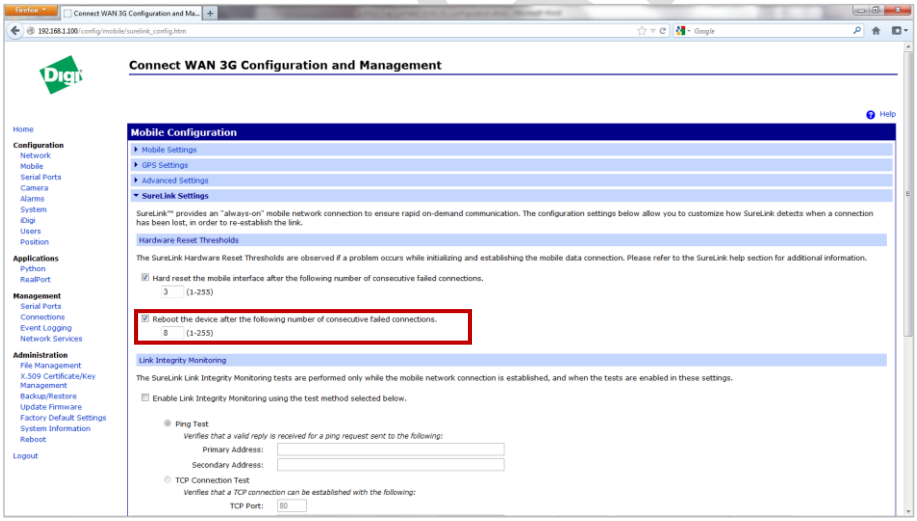
8. On the “Connect WAN 3G Configuration and Management, System Information” screen, click on the “Mobile” link on the left side of the screen under “Configuration.”



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.



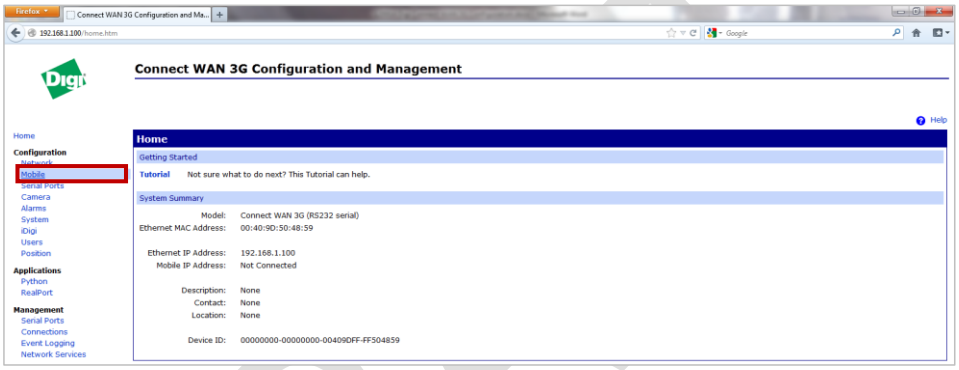
11. Scroll down and click on the “Apply” button.
12. Your backhaul modem is configured and ready for use.

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

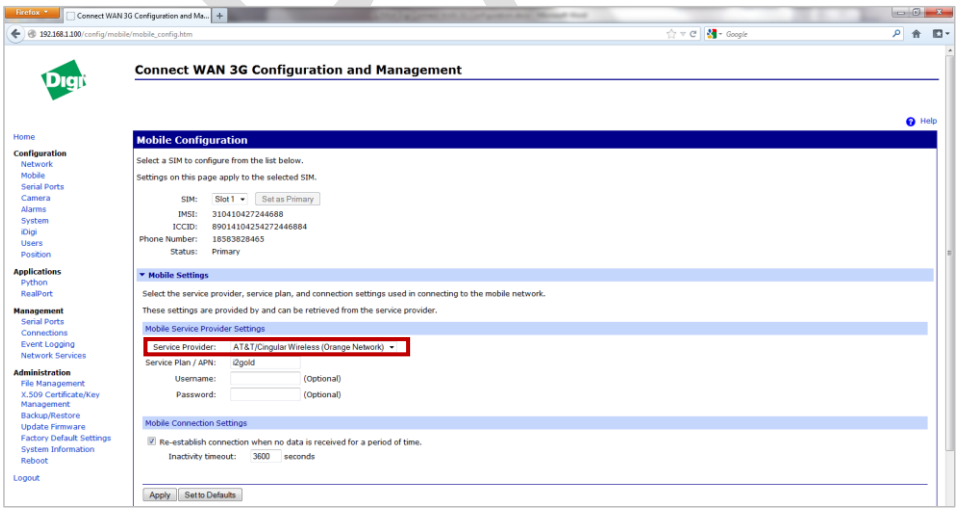
3.4 Mobile Configuration for a GSM/UMTS/HSPA Wireless Carriers

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."

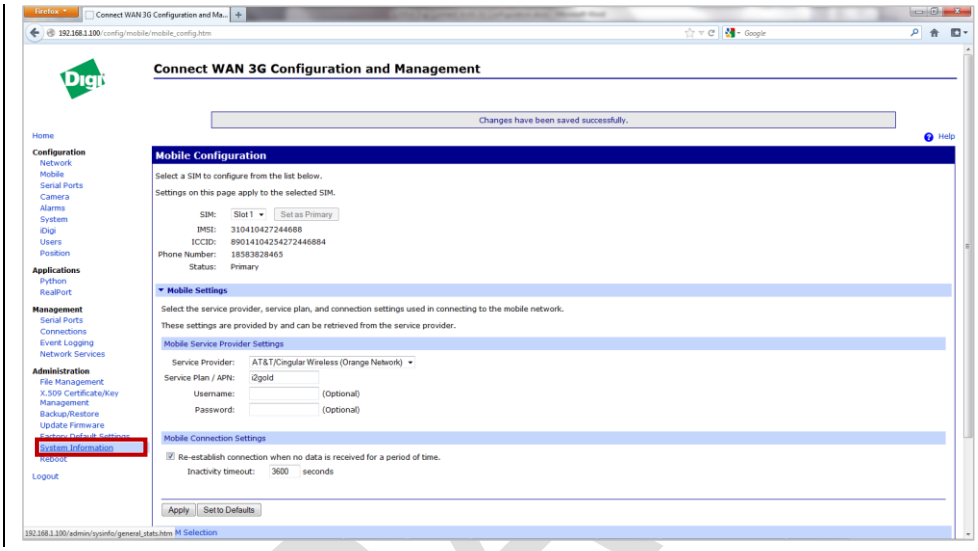


3. From the "Digi Connect WAN 3G Configuration and Management, Mobile Configuration" screen, choose your wireless carrier from the "Service Provider" pull down menu.

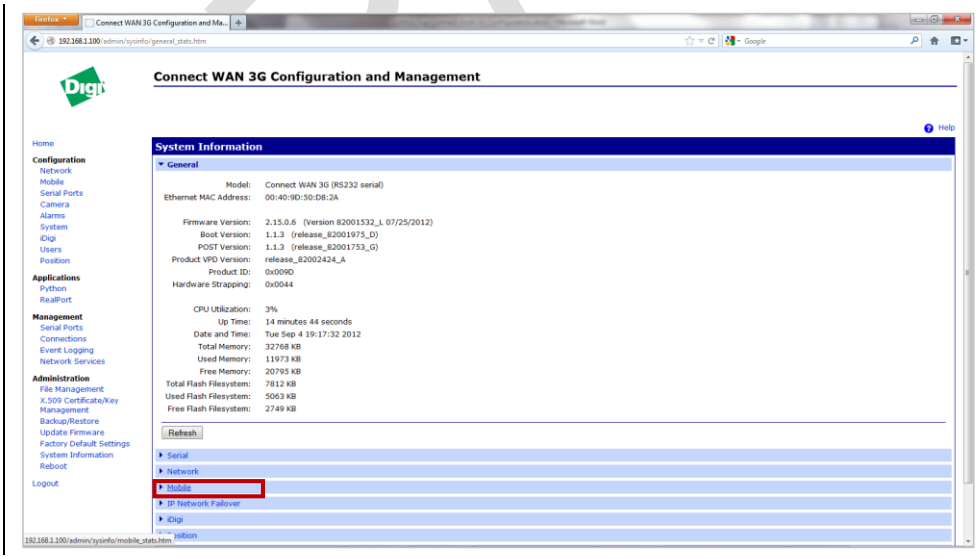


4. From the “Digi Connect WAN 3G Configuration and Management, Mobile Configuration” screen, enter your “Service Plan/APN” and click “Apply.”

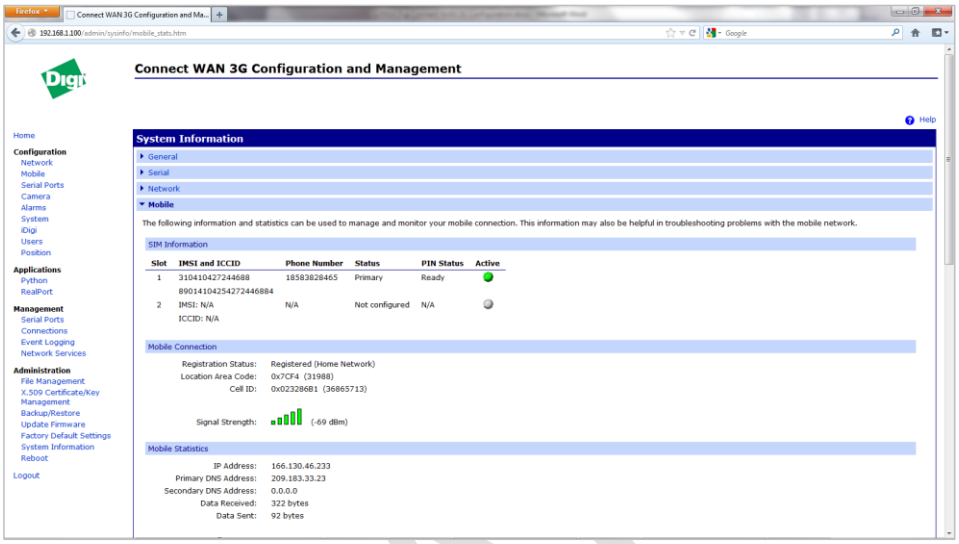
5. Click on the “System Information” link on the left side of the screen under “Administration.”



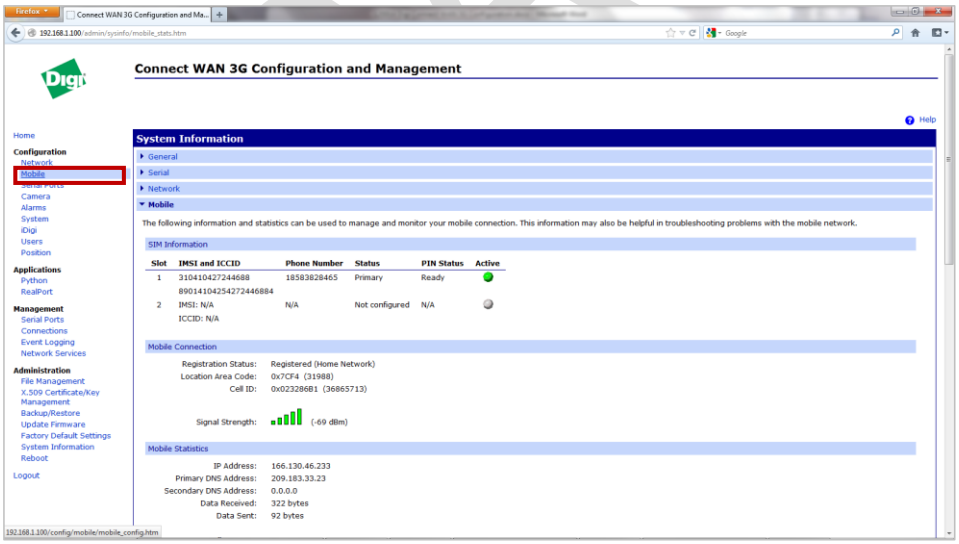
6. Click on the “Mobile” link located on the lower part of the “Connect WAN 3G Configuration and Management, System Information” screen.



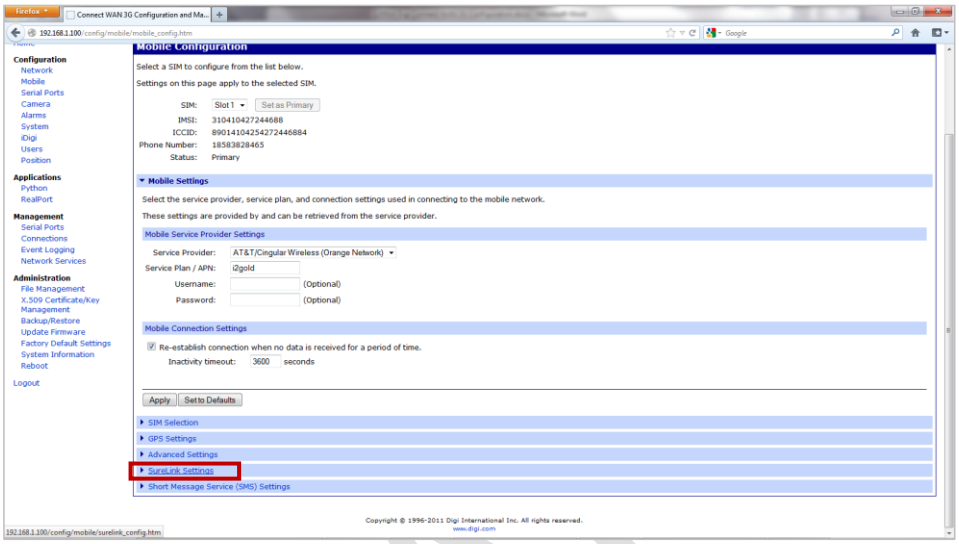
7. Verify that your mobile information is correct.



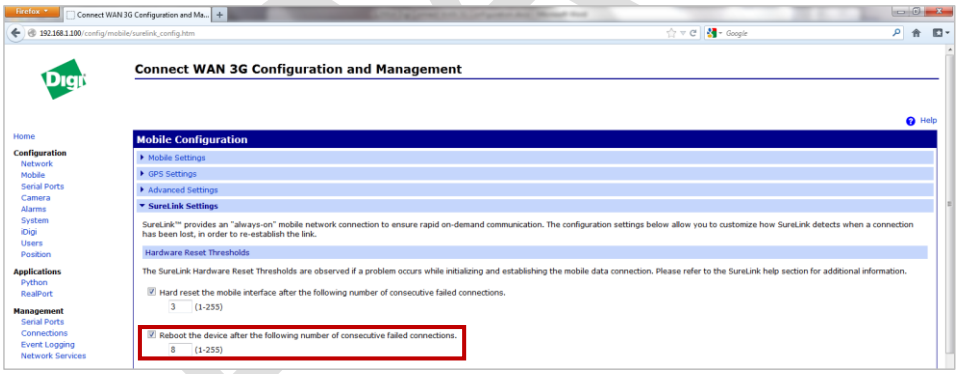
8. On the “Connect WAN 3G Configuration and Management, System Information” screen, click on the “Mobile” link on the left side of under “Configuration.”



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.

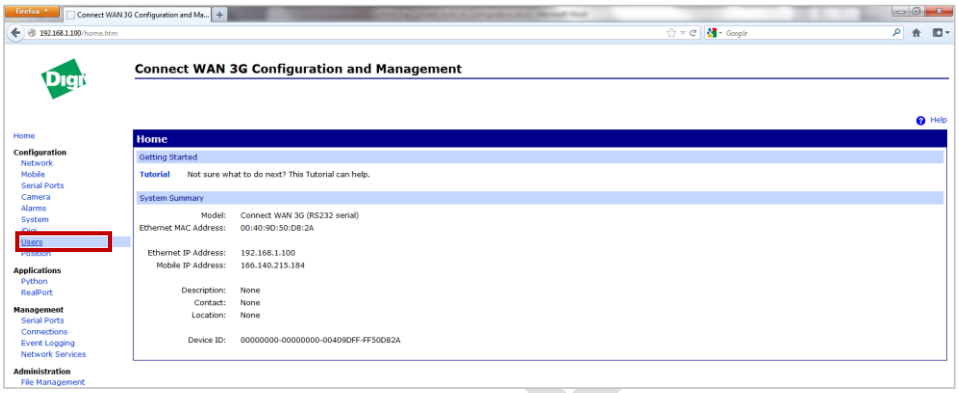


11. Scroll down and click on the “Apply” button. Your backhaul modem is configured and ready for use.

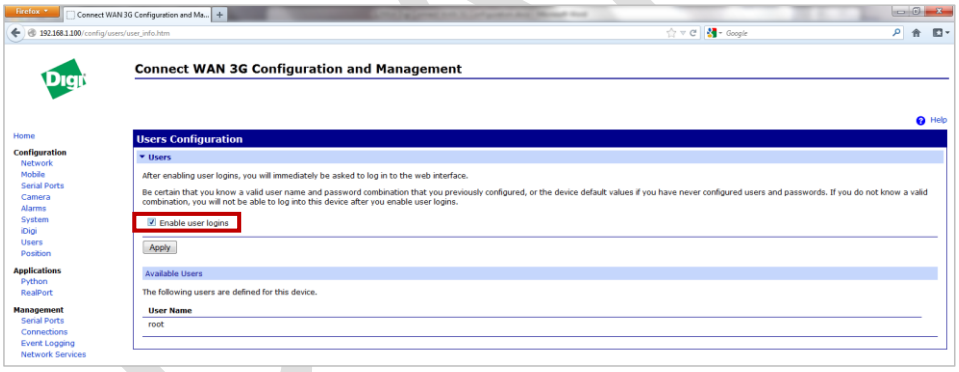
NOTE: Users are strongly encouraged to follow the basic security settings that follow the Mobile Configuration steps.

3.5 Basic Security Settings

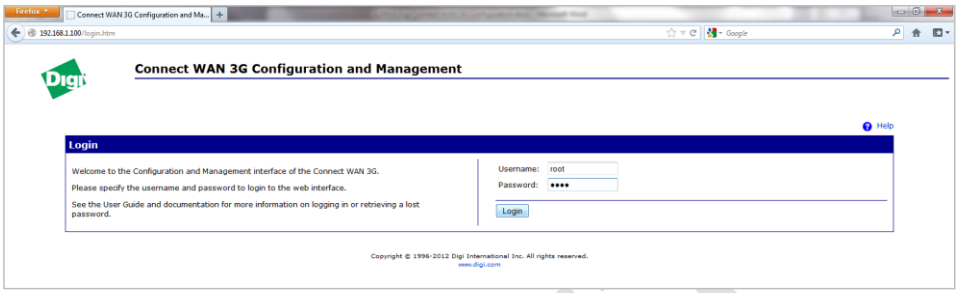
1. From the “Digi Connect WAN 3G Configuration and Management, Home” screen, click on the “Users” link on the left side of the screen under “Configuration.”



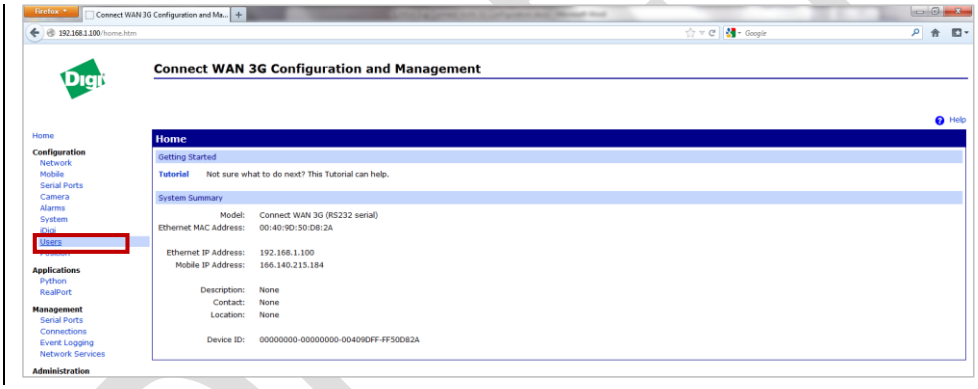
2. From the “Digi Connect WAN 3G Configuration and Management, Users Configuration” screen, check the box for “Enable user logins” and click the “Apply” button.



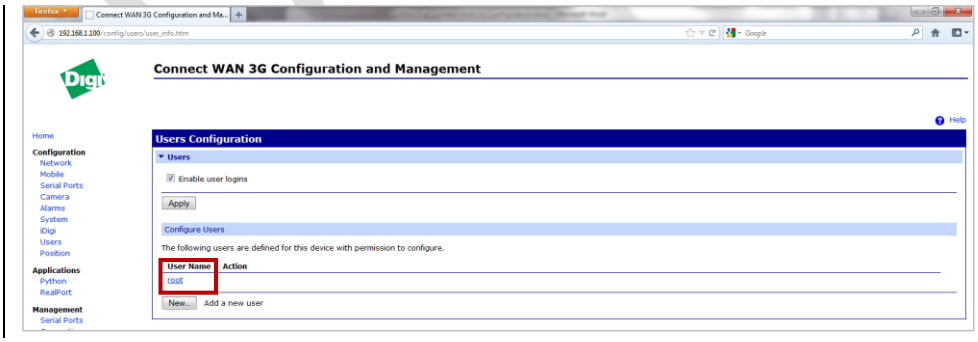
3. On the “Digi Connect WAN 3G Configuration and Management” Login screen, log in with username: root and default password: dbps.



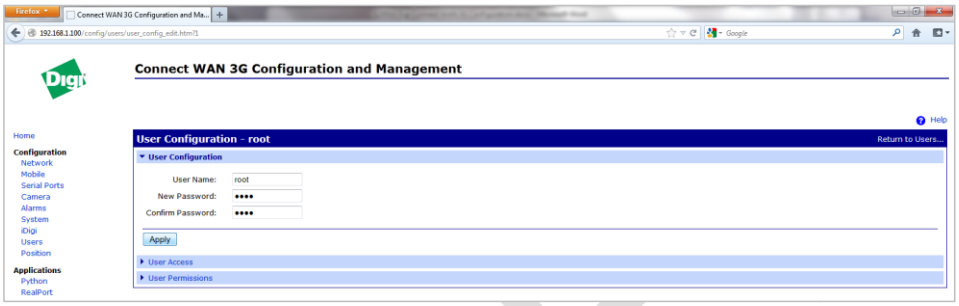
4. From the “Digi Connect WAN 3G Configuration and Management, Home” screen, click on the “Users” link on the left side of the screen under “Configuration.”



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



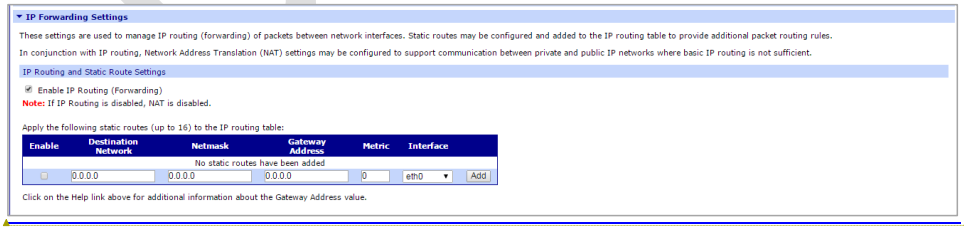
6. From the "Digi Connect WAN 3G Configuration and Management, User Configuration – root" screen, do the following:
   - ❒ Click change and confirm that the "root" password meets or exceeds your company's requirements.
   - ❒ Click on the "Apply" button.



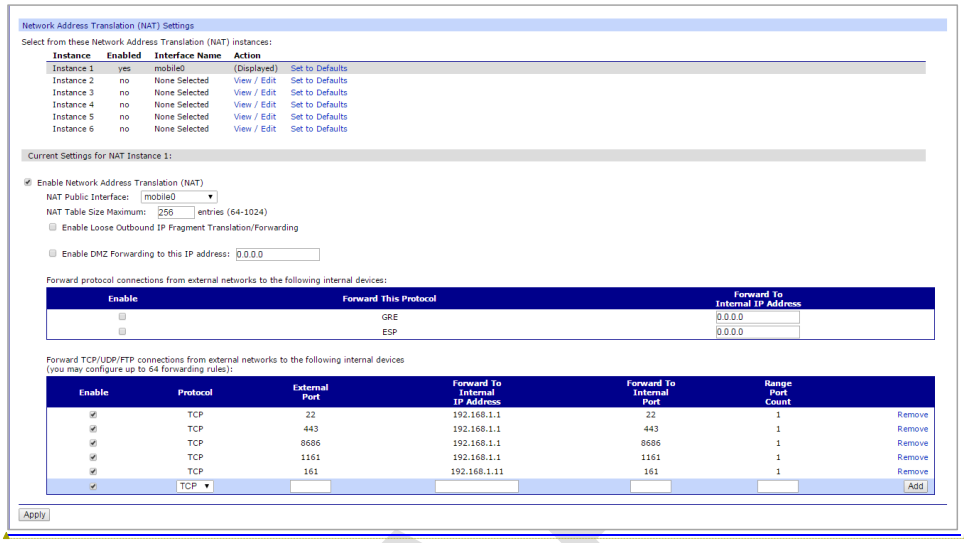
7. For additional security settings, contact you On-Ramp Wireless representative with root access information so that we may configure IP filtering and additional security settings appropriate for your configuration.
8. Refer to Chapter 4: Connecting the AP to the RPMA Network.

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



Formatted: Font: Calibri



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.onrampwirerless.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.

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