AirPrime WP Series

Preparing Your Devices For Deployment

41110380
Rev 1

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless modem are used in a normal manner with a well-constructed network, the Sierra Wireless modem should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless modem, or for failure of the Sierra Wireless modem to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless modem in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the Sierra Wireless modem **MUST BE POWERED OFF**. The Sierra Wireless modem can transmit signals that could interfere with this equipment.

Do not operate the Sierra Wireless modem in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless modem **MUST BE POWERED OFF**. When operating, the Sierra Wireless modem can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless modems may be used at this time.

The driver or operator of any vehicle should not operate the Sierra Wireless modem while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product may contain technology developed by or for Sierra Wireless Inc. This product includes technology licensed from QUALCOMM®. This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from MMP Portfolio Licensing.

Copyright

Trademarks

Sierra Wireless®, AirPrime®, AirLink®, AirVantage® and the Sierra Wireless logo are registered trademarks of Sierra Wireless, Inc.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.

Contact Information

Sales information and technical support, including warranty and returns	Web: sierrawireless.com/company/contact-us/ Global toll-free number: 1-877-687-7795 6:00 am to 6:00 pm PST
Corporate and product information	Web: sierrawireless.com

Revision History

Revision number	Release date	Changes
1	July 2017	Created

Contents

1: Introduction

This document describes configuration recommendations for deploying devices that incorporate WP-series modules, and for WP-series modules obtained directly from distributors. These recommendations are intended to ensure WP-series modules are adequately secured and configured to run properly.

1.1 Factory Configuration vs. Deployment Configuration

WP-series modules are factory-configured with a standard development configuration. This configuration is designed to support device developers/integrators with certain development features enabled and several interfaces available.

The factory configuration is not recommended for devices deployed commercially—devices must be secured for real-world use, development-specific features may negatively affect real-world module performance, etc.

Important: *Sierra Wireless strongly recommends that modules be appropriately configured prior to deployment.*

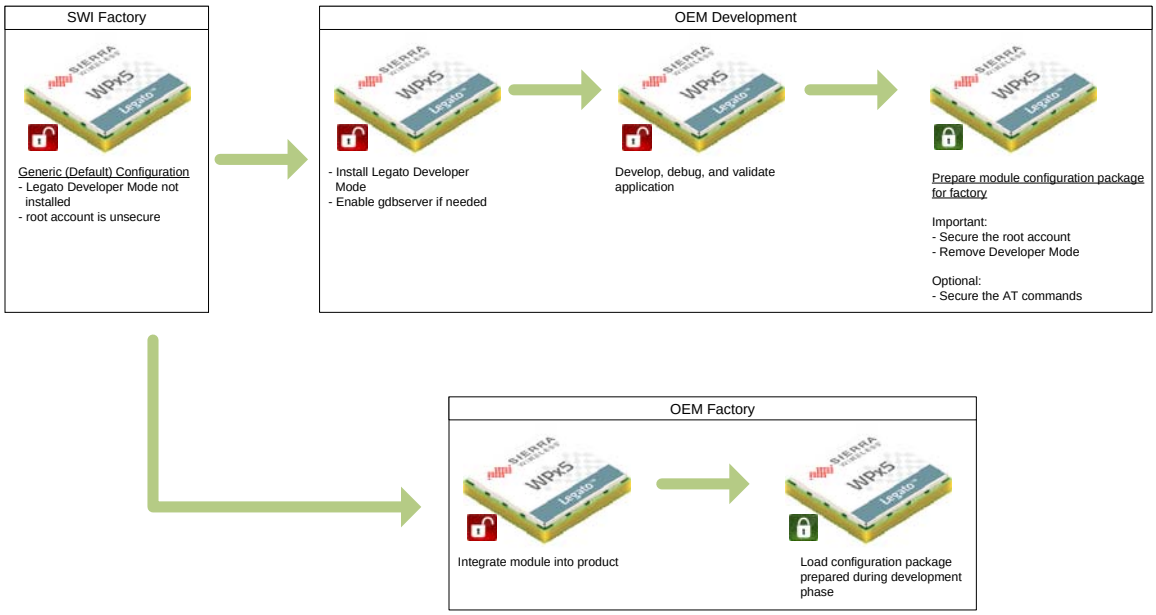

Figure 1-1: Configuration Process—Factory Through Deployment (as of Legato AF 16.10.3 (Release 14))

1.2 Deployment Configuration Recommendations

Several factory configuration elements should be considered prior to deployment, including:

- Module security—Modules should be secured with an appropriate combination of passwords, keys, feature restrictions, etc. (Securing WP Modules on page 9)
- Linux and Legato Application Framework (AF) features—Disable functionality that is intended for use by developers. (Linux and Legato Application Framework on page 18)
- Module firmware—Load or build Sierra Wireless-provided firmware updates, or update and/or load custom firmware images if required. (Firmware Images on page 8)
- Prepare modules for specific carriers—Apply carrier-specific configurations to modules. (Mobile Network Provider-specific Device Configurations on page 21)
- AirVantage—Configure AirVantage-specific functionality as required. (AirVantage Configuration on page 22)

Note: These configuration adjustments are suggestions only and are not to be considered an exhaustive list—the final determination of which adjustments to make is the responsibility of the manufacturer of devices incorporating WP-series modules, or the purchasers of factory-configured modules direct from distributors.

1.2.1 Deploying Bit-pipe Modules

When deploying WP modules for bit-pipe use (using the modem, but not using the application processor), make sure to do the following when preparing the modules in Configure for Deployment on page 7:

- Disable the root account
- Disable or remove Legato AF Developer Mode
- Secure AT command access
- Disable unused UART interfaces
- Disable the ECM USB interface

1.3 Configure for Deployment

When preparing WP-series modules for end-user use, use the following procedure to identify configuration details that may need to be updated (either through dynamic customization changes, or rebuilding the Linux kernel and/or Legato AF):

1. Configure the module's security features—Provide an appropriate level of security for access and use of the module:
   - **a.** If the module should only be accessible by specific devices:
     - **i.** Use SSH Keys on page 13 to give access only to those devices.
     - **ii.** Limit Interfaces that Permit SSH Access on page 15.
   - **b.** To reduce the potential for hardware hacking, disable any interfaces that are not required for deployed use:
     - Disable Unused UART Interfaces on page 14.
     - Disable Unused USB Interfaces on page 14.
   - **c.** Set a password to prevent unauthorized (and potentially harmful) use of 'extended' AT commands—Secure Access to Extended AT Commands on page 15.
     (The development configuration uses a simple, non-unique password that is insufficient for deployment.)

d. Provide the root account with the appropriate level of security required for end-user use of the module:

- If access to the root account will never be required, Disable the Root Account on page 16. (Note: Bit-pipe modules should always have the root account disabled.)

  or

- If some users may require access to root:

  i. Change the Root Password on page 16.

  ii. Control Root Access From Specific TTY Devices on page 17.

2. Remove unneeded developer-specific features—Remove/disable features that are not typically intended for use after deployment:

a. Disable or Remove Developer Mode for Deployment on page 19. Legato AF Developer Mode (if installed and enabled) provides useful features for OEM developers. However, Developer Mode prevents the module from entering sleep mode, which increases power consumption, and increases local network traffic because it keeps trying to connect to Developer Studio on the host. Thus Developer Mode should typically be disabled or removed for deployment.

Note: Typically, bit-pipe modules should have Developer Mode removed.

b. Disable gdbserver on page 20. gdbserver can be used by developers for debugging, but should be disabled /removed before deployment, otherwise the delivered product may be subject to GPLv3 license requirements. (In Legato AF 16.10.3 (Release 14), gdbserver is included in Developer Mode. In earlier releases, it is part of the Linux distribution.)

3. Apply any required carrier-specific configurations—If the module will be used on the AT&T network, Configure for AT&T on page 21.

4. Apply AirVantage configurations—If the module will be used with AirVantage, make sure the device is registered on AirVantage, and Enable/Disable AV Polling on page 22 based on the end-user's requirements.

1.4 Firmware Images

If your deployment requires a customized build of the Sierra Wireless Linux distribution and/or Legato AF, you can build your own images and load them onto the module.

For details, refer to the AirPrime WP Flash Guide, available at http://source.sierrawireless.com/resources/#tags=WP Flash Guide.

2: Securing WP Modules

WP-series modules are factory-configured for developer use with specific interfaces enabled and minimal security.

Sierra Wireless recommends that you secure the WP module prior to deploying devices with integrated modules or using factory-configured modules obtained from distributors. Several methods can be used that apply to the module's physical interfaces and access (local/remote) to the root account.

Figure 2-1 on page 9 illustrates the WP module's default configuration and architecture/interfaces that the security methods in Table 2-1 on page 10 can affect.

Note: Configure for Deployment on page 7 provides a recommended process for ensuring all deployment configurations (including security) are considered.

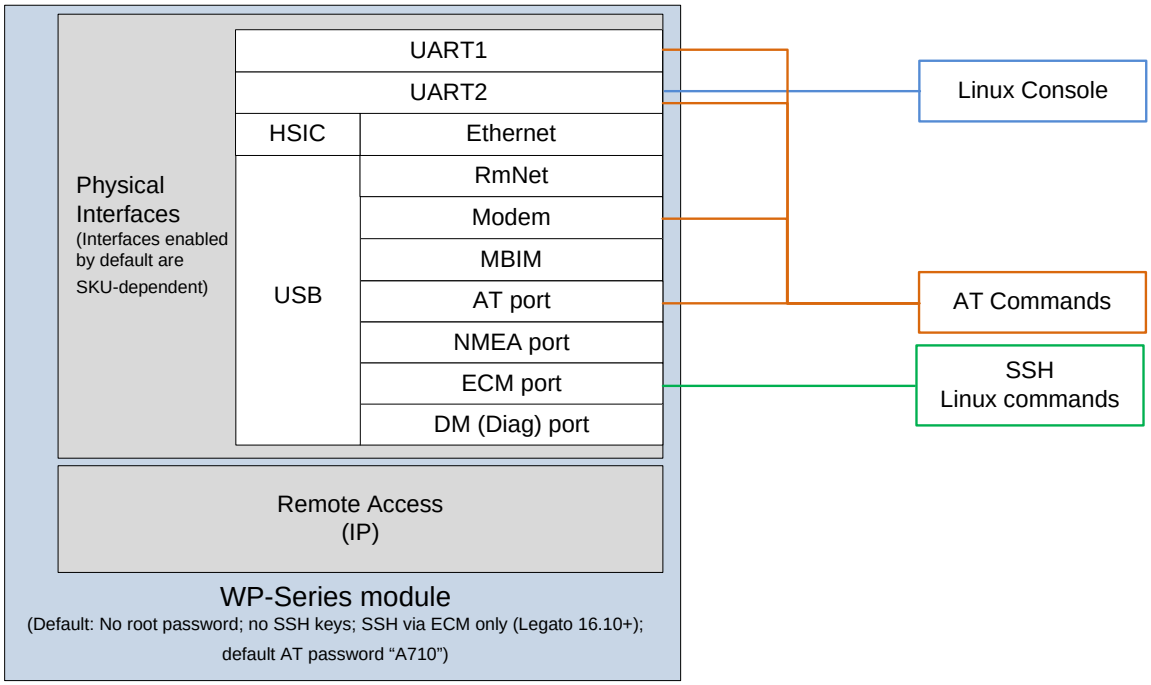

Figure 2-1: Default WP-series Module Configuration

Table 2-1: WP-series Module Security Considerations

Security Method	Description
Secure SSH access Importance—Strongly recommended Type—Command level	Defaults: • Module is not provisioned with SSH keys • On Legato AF 16.10 (Release 13) and later, SSH access is limited by default to only the ECM interface. Risk-Module can be accessed by unknown host devices/users. Recommendations: • Good—Restrict SSH access to local interfaces (see 2.5 Limit Interfaces that Permit SSH Access on page 15) • Better—Also disable password login and use SSH keys (see 2.2 Use SSH Keys on page 13 and 2.1 Configure the Root Account with Login Nagger on page 12) • Best—Disable SSH if not required (see 2.5 Limit Interfaces that Permit SSH Access on page 15) Effect—Access is restricted to specific devices/users, or is prevented completely.
Disable unused UART interfaces Importance—Recommended Type—Interface level	Default—Default UART1/UART2 states are SKU-dependent. Risk—Potential risk of hardware hacking via direct connection to the UART serial interface(s). Recommendation—Disable one or both UART interfaces if they are not being used. Effect—Prevents access to the disabled interface(s). For details, see: • 2.3.1 Disable Unused UART Interfaces on page 14
Disable unused USB interfaces Importance—Recommended Type—Interface level	Default—Default USB interface states are SKU-dependent. Risk—Unknown Recommendation—Disable any USB interfaces that are not required. Effect—Eliminate potential attack vectors. Unused USB interfaces are not enumerated to the host. For details, see: • 2.3.2 Disable Unused USB Interfaces on page 14
Change password for extended AT commands. Importance—Strongly recommended Type—Command level	Default—All modules are factory-provisioned with a default password ("A710") to access extended AT commands. Risk—Incorrect use of extended AT commands can make the platform unstable or unusable. Recommendations: • Good—Strong password unique to the organization • Better—Strong password unique to the device • Best—Strong password unique to the device and randomly generated Effect—Unauthorized users are prevented from using extended commands For details, see 2.4 Secure Access to Extended AT Commands on page 15.

Table 2-1: WP-series Module Security Considerations (Continued)

Security Method	Description
Set root password Importance—Strongly recommended Type—Command level	Default—Modules are factory-provisioned without a root password. Risk—Uncontrolled access to root functionality (e.g. IP traffic could be intercepted (snooping), altered, or blocked) Recommendations: • Minimum—Any password • Good—Strong password unique to the organization • Better—Strong password unique to the device • Best—Strong password unique to the device and randomly generated Effect—Prevent uncontrolled root access For details, see • 2.6.1 Change the Root Password on page 16 • 2.1 Configure the Root Account with Login Nagger on page 12 (Legato AF 16.10+ (Release 13+) only)
Limit root access Importance—Strongly recommended Type—Command and interface level	Defaults: • All connected devices can access the root account via direct login or SSH. (The file /etc/securetty does not exist.) • Root account is enabled • On Legato AF 16.10 (Release 13) and later, SSH access is limited by default to only the ECM interface. Risk-root can be accessed by unknown host devices/users. Recommendations: • Good—Restrict root login to specific devices via /etc/securetty (see 2.6.3 Control Root Access From Specific TTY Devices on page 17) • Better—Disable root login and ssh (see 2.6.3 Control Root Access From Specific TTY Devices on page 17 and 2.5 Limit Interfaces that Permit SSH Access on page 15) • Best—Disable the root account (see 2.6.2 Disable the Root Account on page 16) Effect—Root access is restricted to specific devices, or not allowed.
Disable Linux serial console access Importance—Optional Type—Interface level	Default—Console is enabled. Risk—Unauthorized access to module. Recommendation—Disable console if it is not required. (Requires the kernel to be rebuilt with appropriate options configured. Refer to appropriate online resources for suggested options.) Effect—Cannot log in via the console, and console output cannot be viewed. Refer to appropriate online resources for suggested options

2.1 Configure the Root Account with Login Nagger

Note: This topic applies only to Release 13 (Legato AF 16.10.0 and Linux distribution SWI9X15Y_07.11.21.00), or later. Earlier versions of Legato AF do not have the login nagger—passwords and ssh keys must be set manually from the Linux shell.

The first time you log in to the module (target) as root, using a serial console or SSH connection, a 'login nagger' menu displays a list of setup options to configure the root account's remote login security method. (If additional options are added, some of the option numbers described below may change.)

```
1—Setup SSH keys and disable passwords-based authentication via ssh
(the most secure).
Note: Sierra Wireless strongly recommends you select this option
since it provides the greatest remote login security.
2—Setup password (better than nothing).
3—Do nothing.
```

When the menu appears:

1. Select the security method you want to use.
   - 1-Setup SSH keys ...—A second list of options appears with instructions to set up the host. When this appears:
     i. Follow the procedure in Use SSH Keys on page 13 to set up the SSH keys.

     The nagger will not appear on future login attempts.

     Important: *Before logging out from all connected terminals, make sure to test the new SSH keys to be sure you don't lose access to the target device.*
   - 2-Setup password ...—A prompt appears to enter a new root password:
     i. Follow the prompts to enter a new password for root.
     ii. When prompted to disable console access, select Y to disable or N to enable console access.

     Warning: *If you disable console access, the only way to connect to root will be via ssh. Otherwise, root will be inaccessible.*

     If the password was set up successfully, the nagger will not appear on future login attempts.

     Important: *Before logging out from all connected terminals, make sure to test the new password to be sure you don't lose access to the target device.*
   - 3-Do nothing—A prompt appears asking if the nagger should appear again:
     i. Select Y to display the nagger on the next login attempt, or N to stop displaying it.

     (Note: If you want to set optional password settings (set expiry period, display warnings before expiring, force expired accounts to be deactivated), choose the option to do nothing, and then Follow the procedure in Change the Root Password on page 16.)

2.2 Use SSH Keys

Recommendation: If only specific machines should be able to access the target, set up SSH keys for each of those machines.

When you set up SSH keys, consider the following recommendations:

- Create different keys for each device.
- Use a single, strong pass-phrase to protect the ssh private keys on a single host. This allows use of unique keys for each device, and user must remember only a single pass-phrase.
- Keep a secure backup copy of the ssh keys on separate media (e.g. flash drive, tape, etc.) for use if the host machine fails.

To set up SSH keys:

1. On the development machine (host), set up the ssh keys using one of the following methods:
   - Method 1—Use the configtargetssh configuration tool:
     i. Set up Legato AF shell variables:
        ```
        $ . bin/legs
        ```
     ii. Create the SSH key and copy it to the target:
        ```
        $ configtargetssh <device_IP>
        ```
        (For example, <device_IP> is 192.168.2.2 for a device connected over USB, but could be different if connected over Ethernet.)
     iii. When prompted to enter a passphrase (to protect the ssh keys), enter an appropriate passphrase (or leave blank for no passphrase).

     Warning: *If you forget the passphrase, you will no longer be able to access the target from the development machine.*

     iv. When prompted for the target's root password, enter the current password (or press Enter if there is no root password).
     The new ssh keys are automatically set up on the target.
     v. Exit from the target.
     vi. On the development machine, make sure you can log in to the target using the ssh keys:
        ```
        $ ssh 192.168.2.2
        ```
        (You do not have to enter a user name or password)
   - Method 2—Manually set up SSH keys using ssh-keygen.
2. If you:
   - Started this procedure from the login nagger (Configure the Root Account with Login Nagger on page 12):
     i. Go back to the screen that was showing the nagger menus and select "1) Done setting up my ssh keys".
     ii. When asked if you can successfully login using ssh keys, type `Y`.
     A new menu appears with options to configure the local console login.
     iii. Select the option that best fits the customer's requirements and follow the instructions that appear.
   - Did not use the login nagger and want to disable SSH password authentication on the target (which means you will only be able to authenticate using SSH keys):
     i. Open an ssh session to the target.

ii. Disable ssh password authentication:

```
# echo "DROPBEAR_EXTRA_ARGS=\"-s -sg\"" >> /etc/default/dropbear
# /etc/init.d/dropbear restart
```

Important: *Before logging out from all connected terminals, make sure to test the ssh keys to be sure you don't lose access to the target device.*

2.3 Secure the Physical Interfaces

2.3.1 Disable Unused UART Interfaces

Recommendation: Disable any UART interfaces that are not required.

If any UART interfaces are not required, they should be disabled to secure the module against hardware hacking:

1. Log in as root.
2. Use either of the following methods to disable the UART interface(s):
   - Use the AT!MAPUART command:

     `AT!MAPUART=0,1` (Disable UART1)

     `AT!MAPUART=0,2` (Disable UART2)
   - (Legato AF 16.10 or later) Use the Legato AF uartMode command:

     `# uartMode set 1 disable` (Disable UART1)

     `# uartMode set 2 disable` (Disable UART2)

2.3.2 Disable Unused USB Interfaces

Recommendation: Disable any USB interfaces that are not required.

Note: If disabling some or all of the USB interfaces:
• The DM interface cannot be disabled.
• If you want to be able to use fwupdate to update the module, do not disable the ECM interface
• !USBCOMP allows you to disable any two of the following interface: AT, modem, MBIM (at least one must always remain enabled)

To disable unused USB interfaces:

1. Connect to the module's AT COM port.
2. Display all available interfaces using the !USBCOMP AT command:

   `AT!ENTERCND="A710"`

   `AT!USBCOMP?`
3. Determine the bitmask to use that identifies all the interfaces that should be enabled. To display a list of all possible interfaces, use the following command:

   `AT!USBCOMP=?`
4. Set the device's USB interface configuration to the new bitmask (enabled interfaces):

   `AT!USBCOMP=1,1,<Interface bitmask>`

2.4 Secure Access to Extended AT Commands

Recommendation: Set a strong password for extended AT command access.

To prevent unauthorized access of extended AT commands, select a unique password (4–10 alphanumeric characters) to replace the WP module's default password for extended AT commands ("A710").

To change the AT command password:

1. Connect to the module's AT COM port.
2. Enable extended AT command access using the current password, and set a unique password:

   ```
   AT!ENTERCND="A710"
   AT!SETCND=<new_password>
   ```

2.5 Limit Interfaces that Permit SSH Access

Recommendation: Deactivate remote SSH access for interfaces that do not require it.

Linux firmware SWI9X15Y_7.11.21.00 and later (Release 13)

Remote SSH access is deactivated by default on Linux firmware SWI9X15Y_07.11.21.00 and later, via pre-configured iptable templates that are applied at boot.

Linux firmware prior to SWI9X15Y_7.11.21.00 (Release 12 and earlier)

To deactivate remote SSH access on Linux firmware prior to SWI9X15Y_07.11.21.00:

- Set appropriate filters with iptables (for additional details, use "`iptables --help`"), and/or
- Limit dropbear to only monitor a specific IP address:

  a. Determine the IP address of the ECM (usb0) interface (in the example output below, the address is 192.168.2.2):

  ```
  # ifconfig usb0
  usb0  Link encap:Ethernet  HWaddr 6E:99:B8:80:8A:2D
        inet addr:192.168.2.2  Bcast:192.168.2.255  Mask:255.255.255.0
        ...
  ```

  b. Add the ECM IP address to the extra arguments list (DROPBEAR_EXTRA_ARGS) in /etc/default/dropbear using the option "-B -p<ip_address>".

  For example:

  ```
  DROPBEAR_EXTRA_ARGS="-s -sg -B -p192.168.2.2:22"
  ```

Important: *Make sure to include "-B". This allows login to the device using a blank password, which is required when accessing a new module that has not yet had a root password assigned.*

Note: If the ECM IP address changes, make sure to add the new address into the DROPBEAR_EXTRA_ARGS list.

2.6 Secure the Root Account

To prevent unauthorized access to the WP module's root account, use some combination of the following methods:

- Change the default root password to a random password, unique per module.
- For increased security, disable the root account to prevent brute-force hacking attempts to access the module via the root user.
- Control root access from specific tty devices.
- Disable UART interfaces (if not required).

2.6.1 Change the Root Password

Recommendation: Change the root password to a random password, unique per module.

Note: Sierra Wireless strongly recommends that SSH keys be used instead of password authentication since they provide stronger security. To use SSH keys, see *Use SSH Keys on page 13**.*

To change the root password:

1. Log in as root.
2. Use the passwd command to change the password and, for additional security, set the password to expire after a specified number of days (for additional details, use the “man passwd” command):

   ```
   # passwd [-x <expire_days>] [-w <warn_days>] [-i <inactive_days>]
   ```

   Where:

   <expire_days>—Number of days before the password expires and must be changed.

   <warn_days>—Number of days in advance of the password expiring that warning messages begin appearing to change the password.

   <inactive_days>—Number of days after the password expires at which point the account is disabled.

Important: *Before logging from all of the connected terminals, make sure to test the new password to be sure you don’t lose access to the target device.*

2.6.2 Disable the Root Account

Warning: *This should be your final step when configuring the module—when root is disabled, you will not be able to do any other configurations that require root access (such as configuring ports, firewalls, etc.).*

Warning: *Only disable the root account if you are sure root access will not be needed in the future. Once the account is disabled, it cannot be re-enabled.*

To disable the root account:

1. Log in as root.
2. Use the usermod command to disable the account:

   ```
   # usermod -L -e 1
   ```

2.6.3 Control Root Access From Specific TTY Devices

Recommendation: If appropriate, allow root access only from specific tty devices.

The /etc/securetty file identifies all tty devices (interfaces) that can log in to the root account. If only specific tty devices must have access to the root account, edit the file as appropriate.

If all tty devices must be able to access the root account, the file /etc/securetty must not exist. (This is the default configuration.)

If only specific tty devices must have access to the root account:

1. Log in as root.
2. Edit the file /etc/securetty:
   a. Add the tty devices if they are not already listed.
   b. Remove any tty devices that should not have access.

To prevent all tty devices from accessing the root account:

1. While logged in as root, clear the securetty file to indicate no tty devices should have access:

```
# echo > /etc/securetty
```

Examples

- No /etc/securetty—All tty devices can access root.
- Empty /etc/securetty—Root access restricted to single-user mode (or su, sudo, etc.)
- Populated /etc/securetty—Only specified devices can access root. In the sample below, root access is allowed from the console and serial ports ttyS0/ttyS2, but not ttyS1.

```
...
console

# Standard serial ports
ttyS0
# ttyS1
ttyS2
...
```

2.7 Security Examples

2.7.1 Example-Configuring Security for Bit-pipe Usage

The following Linux and Legato AF commands secure access to a WP module that is being used as a 'bit-pipe' only (no applications running) by disabling the root account, preventing root access from any console, and disabling UART interfaces:

1. Log in as root.
2. Enter the following commands:

```
# usermod -L -e 1 root
# echo > /etc/securetty
# uartMode set 1 disable
# uartMode set 2 disable
```

3: Linux and Legato Application Framework

WP-series modules are factory configured with a Linux distribution and the Legato Application Framework (AF) for application development.

As detailed in Table 3-1, certain Linux firmware releases or Legato AF versions include the Developer Mode application, the TCF (Target Communication Framework) agent for Legato AF Developer Studio to 'discover' the module on a network, and the gdbserver application for remote debugging:

- Developer Mode—Provides useful development tools, but typically should not be distributed due to potential impact on power consumption
- TCF Agent—Required for use during development (with Developer Studio), but typically should not be distributed since it is always on, signaling its presence to Developer Studio, resulting in unnecessary network traffic.
- gdbserver—Useful application for remote debugging, but should not be distributed due to licensing issues

Table 3-1 describes where these features are included (Linux firmware or Legato AF) and provides general deployment suggestions/recommendations

Table 3-1: Linux Firmware/Legato AF Deployment Considerations

Linux Firmware→ Legato AF→	Release 12 SWI9X15Y_07.11.21.00 AF < 16.10.0	Release 13 SWI9X15Y_07.11.21.00+ AF 16.10.0	Release 14+ SWI9X15Y_07.12.09.00+ AF 16.10.3+
Features/Considerations			
Developer Mode	n/a	Installed	Available, not installed
TCF Agent	In distro, always on	In distro, always on	In Developer Mode, on while Developer Mode is enabled
gdbserver	In distro, enabled	In distro, enabled	In Developer Mode, disabled
Deployment Suggestions/Recommendations			
	• Upgrade to newer distribution and Legato AF, or • Rebuild distribution (Remove TCF Agent and Disable gdbserver)	• Upgrade to newer distribution and Legato AF, or • Rebuild distribution (Remove TCF Agent and Disable gdbserver), and Disable or Remove Developer Mode for Deployment	Disable or Remove Developer Mode for Deployment

3.1 Developer Mode

The Developer Mode application provides useful features for OEM developers.

Important: *For the latest detailed instructions on installing, enabling, disabling, and removing Developer Mode, go to http://legato.io/legato-docs/latest/basicTargetDevMode.html.*

3.1.1 Enable Developer Mode for Pre-Deployment Development

Developer Mode is available in Legato AF 16.10.0 and later. If you are using an older version of Legato AF, you must update to a newer version to use Developer Mode.

To begin using Developer Mode In Legato AF 16.10.0 and later:

- AF 16.10.3 (Release 14) and later—Developer Mode is available, but not installed on the module. For instructions on building and installing the devMode application, refer to http://legato.io/legato-docs/latest/basicTargetDevMode.html.
- AF 16.10.0 (Release 13)—Developer Mode is factory-installed and enabled on the module, and ready for use.

3.1.2 Disable or Remove Developer Mode for Deployment

If the Developer Mode application is enabled on a deployed module, it will prevent the module from entering sleep mode, which increases power consumption. Also, in Legato AF 16.10.3 (Release 14) and later, the TCF agent will also be running, resulting in increased network traffic.

Thus, when deploying a module, Developer Mode should typically be disabled or removed completely.

Note: If the module is deployed with Developer Mode enabled, make sure to Disable gdbserver on page 20.

To determine if Developer Mode is present on a target device:

- On the target, enter the command:

  # app show devMode

To remove Developer Mode from a single target device:

- On the target, enter the command:

  # app remove devMode

  Note: If Legato AF (16.10.0) is reinstalled later, Developer Mode will also be reinstalled.

To remove Developer Mode from the Legato AF (16.10.0), rebuild the framework with devMode removed in production, before deploying modules (as detailed in http://legato.io/legato-docs/16_10/howToDevMode.html):

1. Remove devMode from the system sdef file.
2. Rebuild the Legato application framework for the target device.

3.1.3 Remove TCF Agent

TCF Agent is required for use during development (with Developer Studio), but typically should not be distributed because it is always on, signaling the module's presence to Developer Studio.

If using Legato AF 16.10.3+, TCF Agent is part of the devMode application, which should be disabled or removed when deploying modules. (See Disable or Remove Developer Mode for Deployment on page 19.)

If using Legato AF 16.10.0 or older, TCF Agent is part of the Linux distribution.

3.2 Disable gdbserver

gdbserver, an application that allows developers to remotely debug the WP device from another system, is included in the Linux distribution (SWI9X15Y_07.11.21.00 (Release 13) and earlier) or in the Developer Mode application (in Legato AF 16.10.3 and later).

Typically, modules should not be deployed with gdbserver enabled, since it is subject to the GNU General Public License (GPLv3), which causes the image to also be subject to GPLv3. If it is not disabled or removed, the end-user's device will also be subject to the GPLv3 license requirements.

To disable gdbserver within Developer Mode:

1. Go to http://legato.io and search for GDB.
2. Locate and follow the topic for debugging using GDB.

To disable gdbserver when it is part of the Linux distribution, you must build a custom Linux distribution with gdbserver removed as a dependency:

- If you do not have your own custom Yocto layers:
  i. Edit the following file:
     meta-swi/common/recipes-core/packagegroups/packagegroup-swi-image-target.bb.
  ii. Comment out the following line to remove the gdbserver dependency:
     RDEPENDS_${PN} += "gdbserver"
  iii. Rebuild the firmware image.
- If you have your own layers:
  i. Create/edit the following file:
     packagegroups/packagegroup-swi-image-target.bbappend
  ii. Add the following line to remove the gdbserver dependency:
     RDEPENDS_${PN}_remove += "gdbserver"
  iii. Rebuild the firmware image.

For details on building a custom firmware image, refer to the AirPrime WP Flash Guide, available at http://source.sierrawireless.com/resources/#tags=WP Flash Guide.

If the Sierra Wireless-provided firmware image(s) for the WP-series module cannot run on your platform, or if you need to add, remove, or modify any features/functionality, you can build your own customer image and load it on the module.

For details, refer to the AirPrime WP Flash Guide, available at http://source.sierrawireless.com/resources/#tags=WP Flash Guide.

4: Mobile Network Provider-specific Device Configurations

Some mobile network providers may require that devices used on their networks have specific configurations or specific approved firmware images.

4.1 Identify Required Firmware Images

To identify the approved firmware images for specific mobile network providers, refer to the module's firmware Customer Release Notes (CRN), available at http://source.sierrawireless.com.

4.2 Configure for AT&T

Devices used on AT&T's network must be configured to comply with AT&T's OMA-DM IMEI Sync (ODIS) service for device identification.

For configuration details, refer to AirPrime - OMA-DM IMEI Sync Guidelines - ODIS - Application Note, available at http://source.sierrawireless.com/resources/#tags=ODIS.

5: AirVantage Configuration

WP-series modules are factory-configured with credentials for AirVantage, which provides device management and FOTA (firmware-over-the-air) services.

If the module is to be used with AirVantage, make sure it is registered on https://airvantage.net.

Note: Certain carriers require that a mechanism be used to push FOTA (Firmware Over The Air) updates to target devices. AirVantage meets these carrier requirements.

5.1 Enable/Disable AV Polling

AV polling is a feature that allows the module to poll (ping) the AirVantage server at a specific interval. When enabled, this establishes a link to the server, which allows the server to initiate services (device monitoring, FOTA, SOTA) as necessary with the module.

Important: *If AV polling is disabled, the AirVantage server will not be 'aware' of the module, and will not be able to initiate data services. If you are concerned about bandwidth usage or periodic uncontrolled transfers, Sierra Wireless advises that AV polling be enabled with a large polling period (interval)—for example, a polling period of 30 days will result in a single monthly connection with minimal overhead (typically less than 2 KB per month).*

AV polling is disabled by default in the factory configuration. Before deploying, make sure the AV polling feature is configured appropriately for customer use.

To disable/enable AV polling:

1. Set the polling period to the desired number of minutes between poll attempts using any of the following methods:
   - AT command—Connect to the module's AT interface and run the following command:

     `AT+WDSC=3,<period>`

     (where <period> = 0 to disable, or 1–525600 minutes)

     Note: This command may return an ERROR until up to 90 seconds after the module boots.

   - Legato APIs—As described in http://legato.io/legato-docs/latest/c_le_avc.html, create and run an application that uses the following APIs;:
     - `le_avc_GetPollingTimer()`
     - `le_avc_SetPollingTimer()`
   - QMI command—Use the QMI request `QMI_SWI_M2M_AVMS_SET_SETTINGS_REQ` in a QMI application. (For QMI development information, refer to Linux QMI SDK Application Developer Guide (Document # 4110914) available at https://source.sierrawireless.com.)

Request — QMI-SWI_M2M_AVMS_SET_SETTINGS_REQ					
Field	**Value**	**Type**	**Parameter**	**Size (bytes)**	**Description**
Type	0x11			1	Polling timer to connect to AirVantage server
Length	4			2	
Value		Uint32	Polling_timer	4	• 0—Disabled • 1-525600 (mins)

2. Log in to your AirVantage account.
3. Refer to https://source.sierrawireless.com/airvantage/avc/reference/monitor/howtos/configureASystemCommunication/ and configure the Heartbeat parameters as appropriate.

6: Abbreviations

Table 6-1: Acronyms and Definitions

Acronym or term	Definition
DM	USB composite diagnostics interface
ECM	Ethernet Control Model—Ethernet emulation over USB
HSIC	High Speed Inter-Chip—USB chip-to-chip interconnect interface
IP	Internet Protocol
MBIM	Mobile Broadband Interface Model
NMEA	National Marine Electronics Association—Refers to frame issued by the GNSS satellite receiver
RmNet	Proprietary USB virtual Ethernet framework developed by Qualcomm
root	Linux administrator account, and access privelege level
SSH	Secure Socket Shell—Network protocol that provides administrators with a secure way to access a remote computer
TTY	Linux terminal device
Yocto	Yocto Project—Tool for creating custom Linux system for embedded products