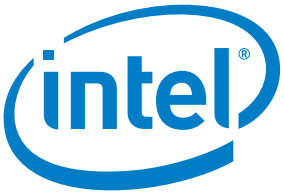


Intel® IoT Gateway Developer Hub and Intel® IoT Gateway Software Suite / Pro Software Suite

Version 3.1.0.18 Production

Release Notes

---

22 August 2016

Document Number: 334680-002
Revision 3.1.0.18

Legal Disclaimers

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting: http://www.intel.com/design/literature.htm

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at http://www.intel.com/ or from the OEM or retailer.

No computer system can be absolutely secure.

Intel, Intel Core processor, Intel Atom processor, Intel Quark processor and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

Wind River is a trademark of Wind River Systems, Inc.

*Other names and brands may be claimed as the property of others.

Revision History

Date	Software Version & Stage	Description
22 August 2016	3.1.0.18 Production Release	Public Release of the latest version of the Intel® IoT Developer Hub and the Intel® IoT Gateway Software Suite/Pro Software Suite, which includes an enhanced sensor UI and configurable lockdown options.
16 July 2016	3.1.0.17 Production Release	Public Release of the Intel® IoT Gateway Software Suite/Pro Software Suite, which includes the Intel® IoT Developer Hub along with the latest version of the Wind River Intelligent Device Platform XT 3.1.
18 April 2016	1.0.2 Production Release	Public Release of the Intel® IoT Developer Hub along with Wind River IDP XT 3 and included in the Intel IoT Gateway Software Suite.

Contents

Figures

Tables

1 Introduction

1.1 Purpose of this Document

This document contains information that is specific to this release of the Intel® IoT Software Suite/Pro Software Suite, which includes the Intel® IoT Developer Hub. The document is comprised of the following:

- Features
- Fixed Issues
- Known Errata
- Changes to Wind River Linux 7
- How to Obtain this Release
- Compatible Hardware and Software

1.2 Intended Audience

This document is intended people who install and/or perform development tasks on the Intel® IoT Developer Hub.

1.3 About the Intel® IoT Gateway Software Suite/Pro Software Suite

The Intel® IoT Gateway Software Suite/Pro Software Suite is a Wind River Linux® operating system that provides leading performance and security for intelligence at the edge, enabling near-real-time analysis and efficient process controls. The Intel® IoT Gateway Software Suite/Pro Software Suite allows access to the Intel® IoT Developer Hub (see section 1.3).

Other features include:

Binary Runtime Images

- The Intel® IoT Gateway Software Suites now are delivered as binary images. These binaries allow us to deliver all of the features of the Software Suite and Pro Software Suite, without you having to recompile a Linux OS image. This helps you get up and running in as little as 10 minutes.

Wind River Intelligent Device Platform XT 3.1

- Comes in two versions, Entry and Pro.
    - The Entry level is delivered as pre-validated base binary image, with no ticketed support or development seats included. It also includes the McAfee* Embedded Control Essential set of security tools.
    - The Pro offers one year of ticketed support, Wind River development tools, and the McAfee Embedded Control Pro set of security tools.

1.4 About the Intel® IoT Developer Hub

The Intel® IoT Developer Hub is a web-based service running on the gateway that allows you to have a hands-on sensor-to-cloud experience in a very short time period. It has built-in tutorials to teach you about tools like the visual programming interface called Node-RED* and the Wind River Helix App Cloud, including sample code to develop the app in the cloud.

The Intel® IoT Developer Hub provides ways to easily manage the administrative settings of the gateway. Sensor data is accessible in two ways:

- Use the Omega temp & humidity sensor included in the Loaner Kit. The Loaner Kit is a 6-month free loaner available from the Demo Depot for customers in the USA, Canada, and the EU. The Loaner Kit contains a gateway and sensor to connect out-of-the box. The temperature Node-RED flow is ready to use and the Kit includes built in tutorials about adding humidity readings via Node-RED.
- Use the previously published recipes & packages to evaluate additional sensors and cloud providers. These are accessible via the Intel® IoT Gateway Developer Hub

The Intel® IoT Developer Hub lets you, as the developer, add packages and develop your apps. When development is complete, you can save a hardened OS image onto a USB flash drive.

Introduced in the spring of 2016, the Intel® IoT Developer Hub gives you these advantages:

Live Dashboard

- Summary view of gateway information
- Graphical view of sensor data
- Notification of available OS updates

Plug and play sensors

- Shows live data from connected sensors
- Easy management of connected sensors via Node-RED

Simple access to repositories and management of popular packages

- Simple to add or remove online package repositories
- Easily list installed packages
- Quickly add, update, or uninstall packages as needed

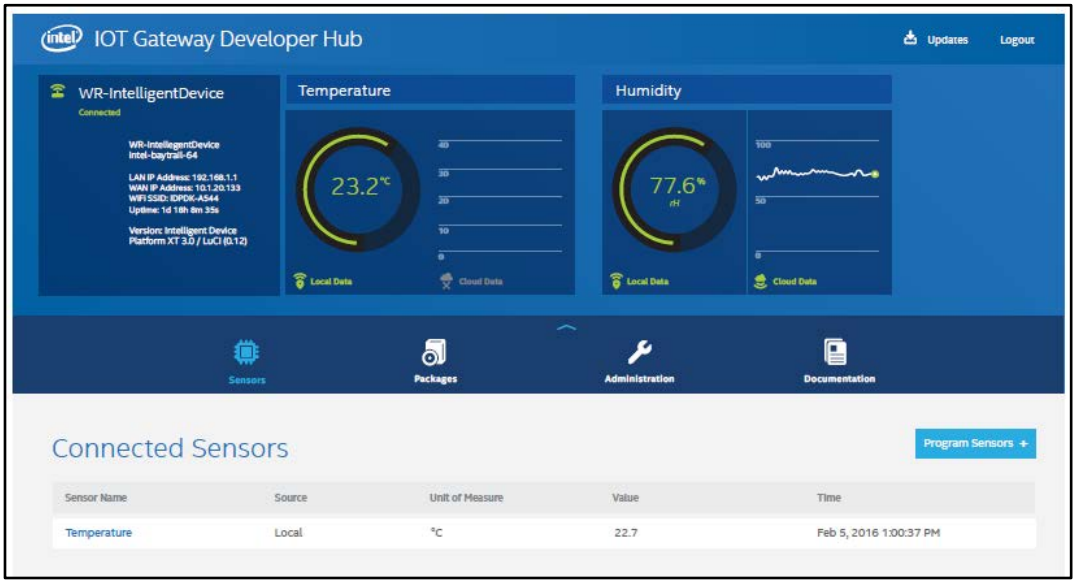
Gateway administration tools and resources

- One-touch buttons for gateway actions including: restart, factory reset, upgrade to Pro, update OS, and change password
- Step-by-step wizard for creating a deployable gateway image
- Direct access to popular development tools including: Node-RED, LuCI*, Cloud Commander*, and Wind River Helix App Cloud*

Clear and simple documentation

- One location to find how-to tutorials and videos, and quick links to key online content

Figure 1. The Intel® IoT Developer Hub User Interface



The Intel® IoT Developer Hub is integrated into the free download of the Intel® IoT Software Suite available at the Intel® IoT Platform Marketplace (IntelIotMarketplace.com).

NOTE: You must **Upgrade to Pro** within the Intel® IoT Gateway Developer Hub interface to utilize the following Pro features:

- McAfee Embedded Control Pro features
- Save a security-hardened, deployable OS image to a USB flash drive
- Legally deploy the generated OS image onto other gateways for pilot or production deployments.

The Pro license is also available from the Intel® IoT Platform Marketplace.

1.5 Related Documents

Technical documentation for Intel® IoT Gateways is online at: http://www.intel.com/gatewaytraining and at https://software.intel.com/en-us/iot/hardware/gateways.

In addition, links to tutorials, templates and guides for the Intel® IoT Developer Hub are included in the user interface, from the **Documentation** tab.

1.6 Technical Support

Free technical support is available on the Intel® IoT Gateway Community Forum (https://communities.intel.com/community/tech/iot-gateway)

Customers who purchase Support Services on the Intel® IoT Platform Marketplace can access their support account and submit support requests at https://customercare.intel.com.

Contact your Intel representative for further assistance.

1.7 Document Conventions

The following conventions are used in this document:

- “Gateway” and “IoT Gateway” refers to any Qualified Intel® IoT Gateway device.
- `This font` is used within paragraph text for code examples, command line entries, API names, parameters, filenames, directory paths, and executables.
- **Bold text** is used for graphical user interface entries and buttons.

2 Features in this Release

This chapter describes the new, changed, and unchanged elements.

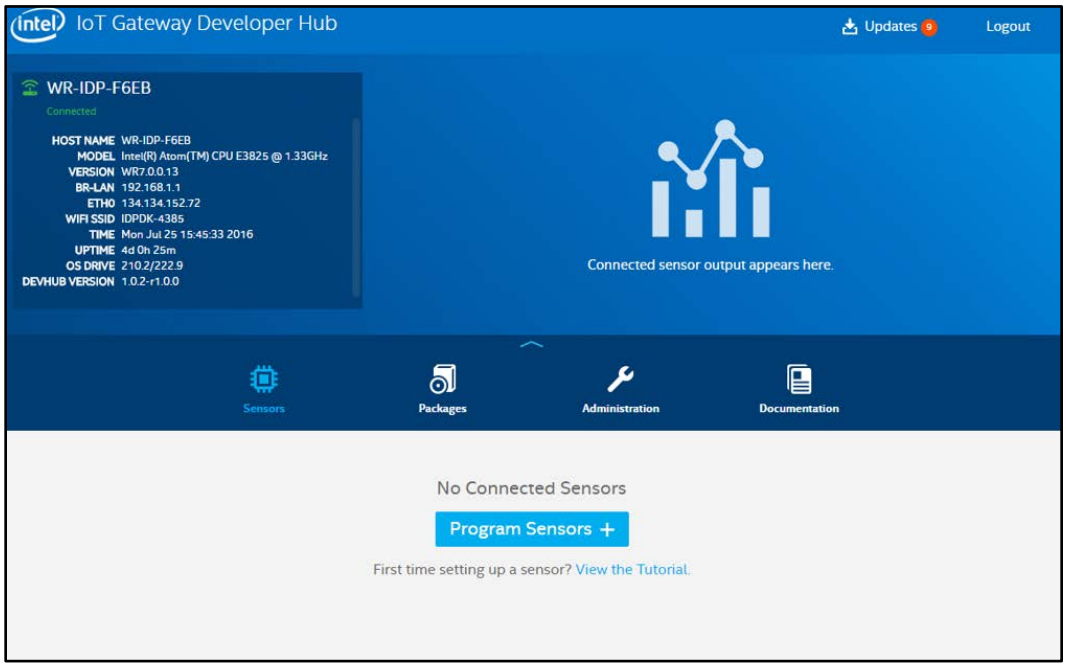
2.1 New Features

2.1.1 Enhanced Sensor User Interface

The enhanced sensor UI makes connecting sensors and viewing data more intuitive. This section outlines the process.

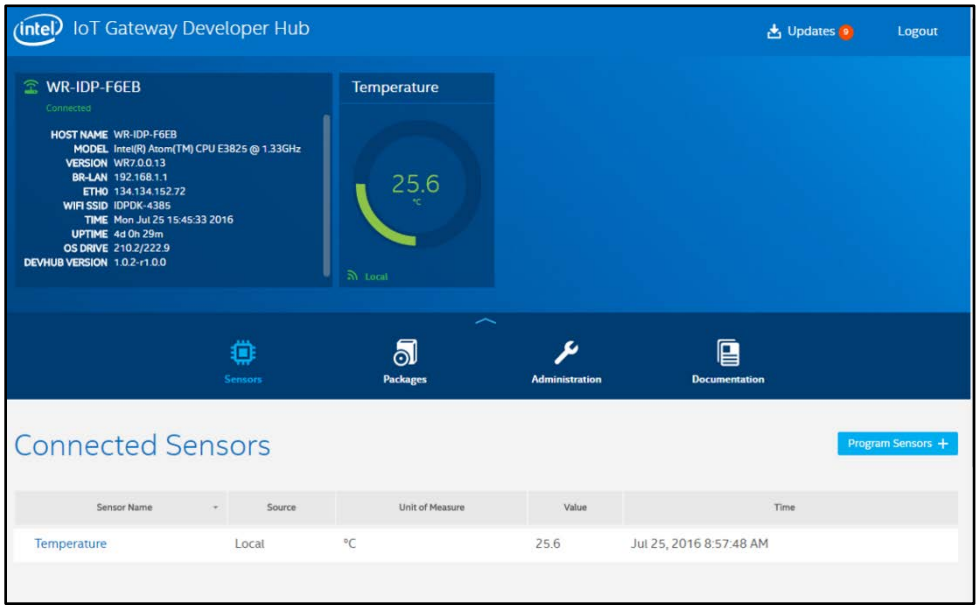
1. Click **Program Sensors +**

Figure 2. Program the Sensors



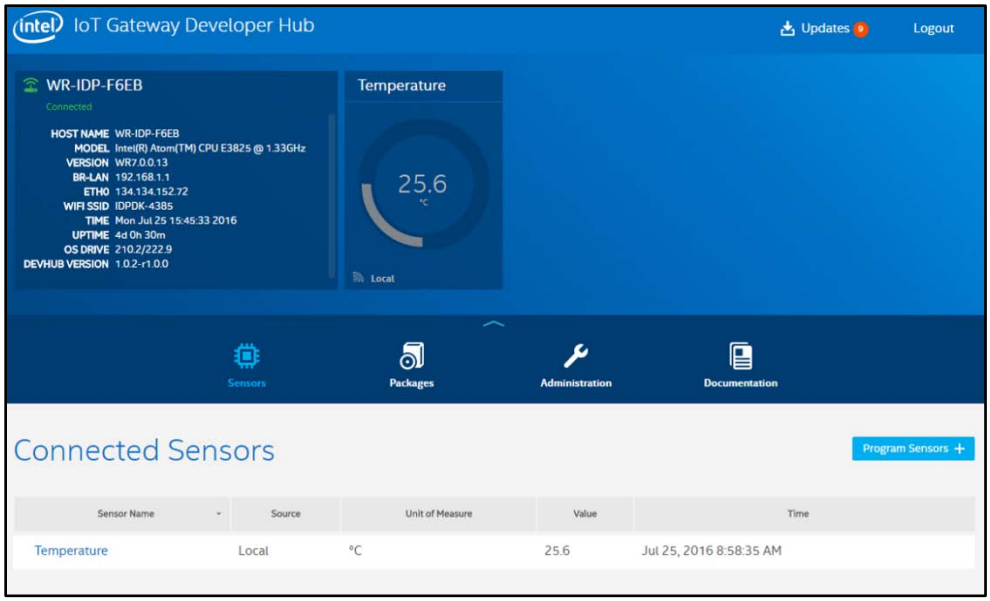
2. Plug in the sensor to the USB port on the gateway. It appears in the dashboard:

Figure 3. Connect the Sensor



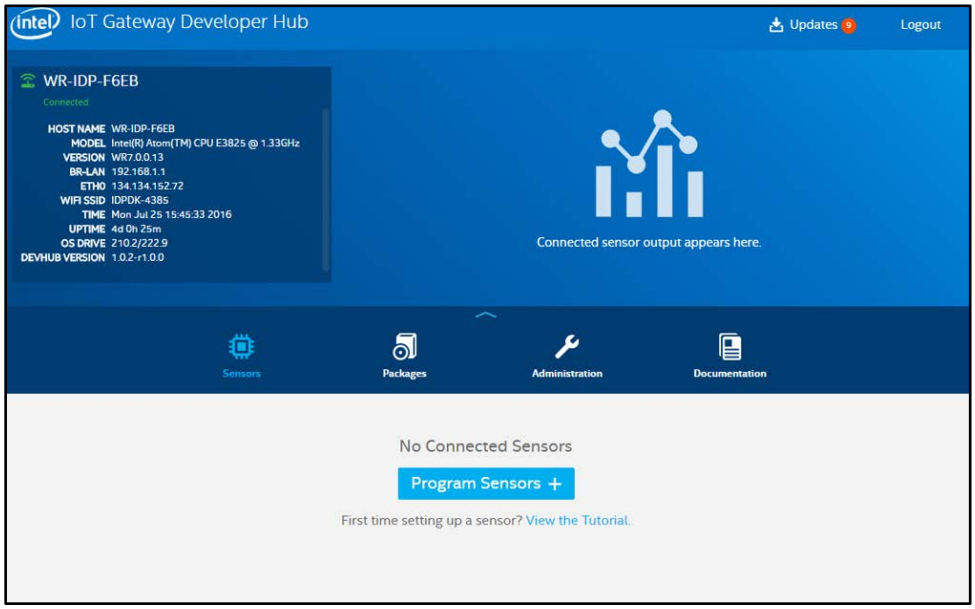
3. Unplug the sensor from the Gateway. The display color for the sensor data changes from green to gray:

Figure 4. Disconnect the Sensor



4. Refresh the page using the command on your browser. The interface shows no connected sensors.

Figure 5. Refresh the Page

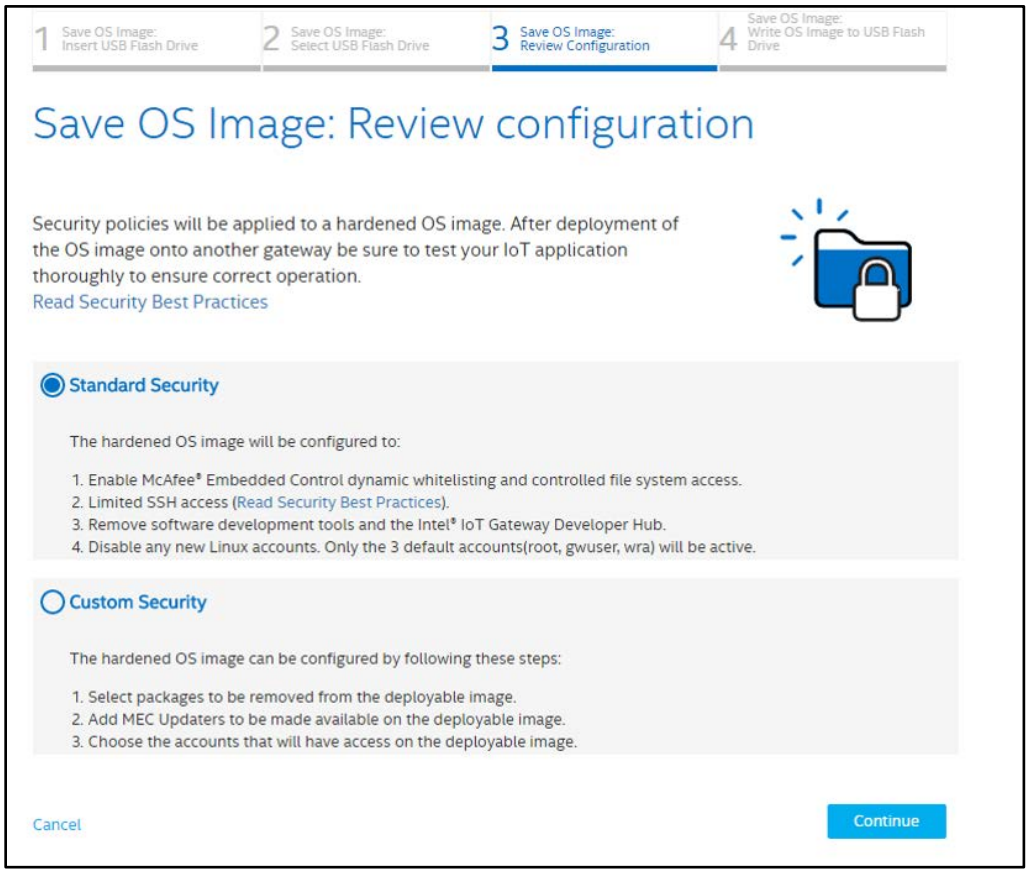


2.1.2 Configurable Lockdown Options

These lockdown options allow you to customize the packages, users, and MEC updaters that you can save to a new locked-down OS image.

Choosing the **Standard Security** option configures the locked down OS image to include the four options shown in Figure 6. Choosing the **Custom Security** option allows you to select specific items to configure.

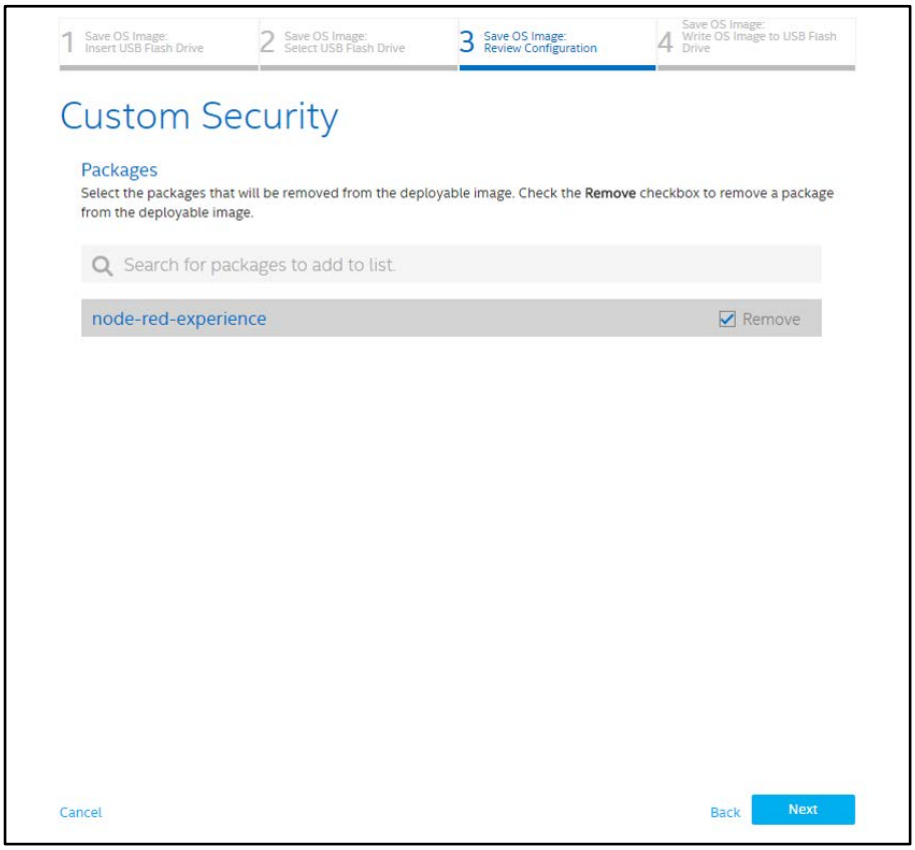
Figure 6. Save OS Image: Review Configuration Page



Click **Continue**.

From the Custom Security page, you can **Search** for packages that you want to remove from the locked down OS image. If you want to include packages in the locked down OS image, remove them from the display list.

Figure 7. Custom Security Page – Packages

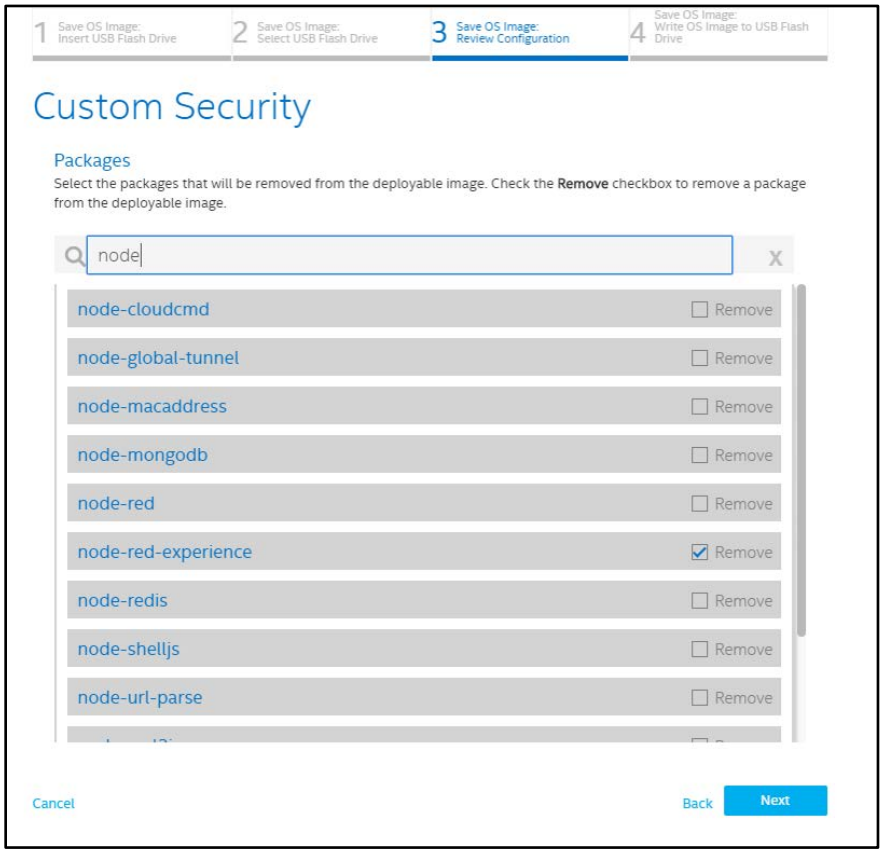


Click **Next.**

These search options are available from the Custom Security page:

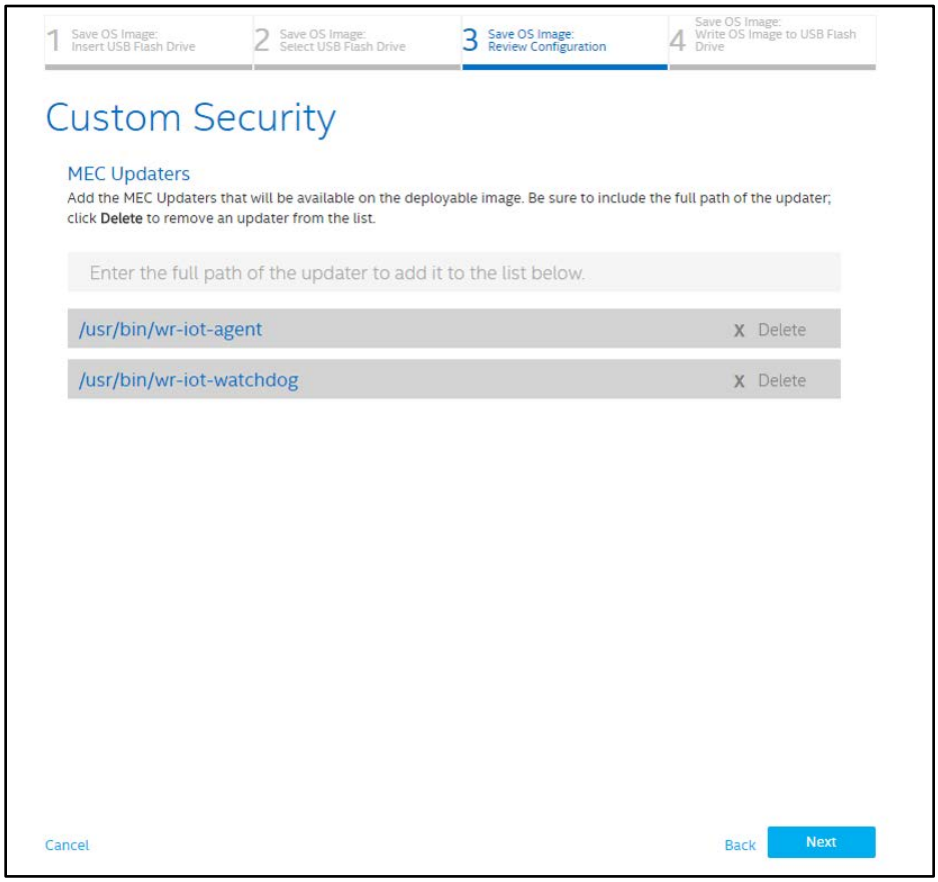
- To perform a search, type your search text into the **Search** field. Press **Enter**.
- To clear the **Search** field, click **X** on the right side of the **Search** field.

Figure 8. Custom Security Page – Searching for Packages



Click **Next**.

Figure 9. Custom Security Page – MEC Updaters



Click **Next.**

You can add or remove MEC Updaters from the locked down OS image as follows

To add an MEC Updater:

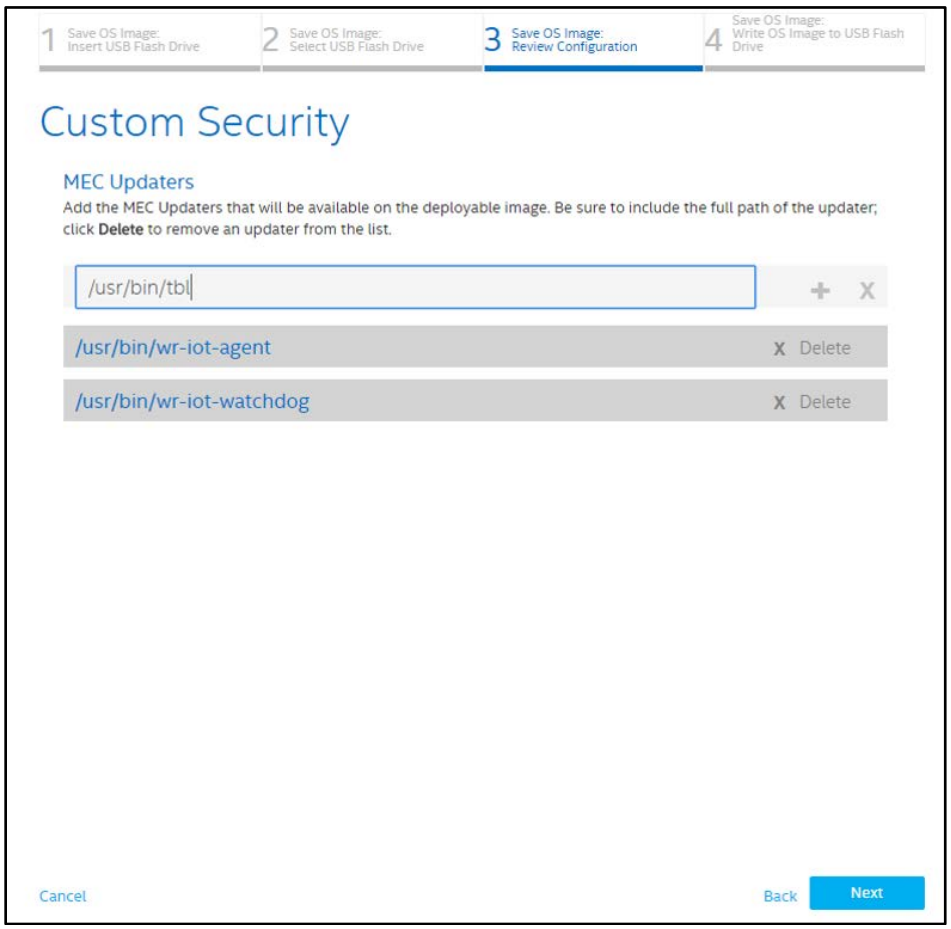
1. Enter the full path of the desired MEC Updater in the field to the left of the **+**.

2. Click **+** to add the MEC Updater to the list.

To clear the search field: Click **X** to the right of the **+**

To remove an MEC Updater: Click the **X Delete** corresponding to the Updater that you want to remove from the locked down OS image.

Figure 10. Custom Security Page – Searching for MEC Updaters

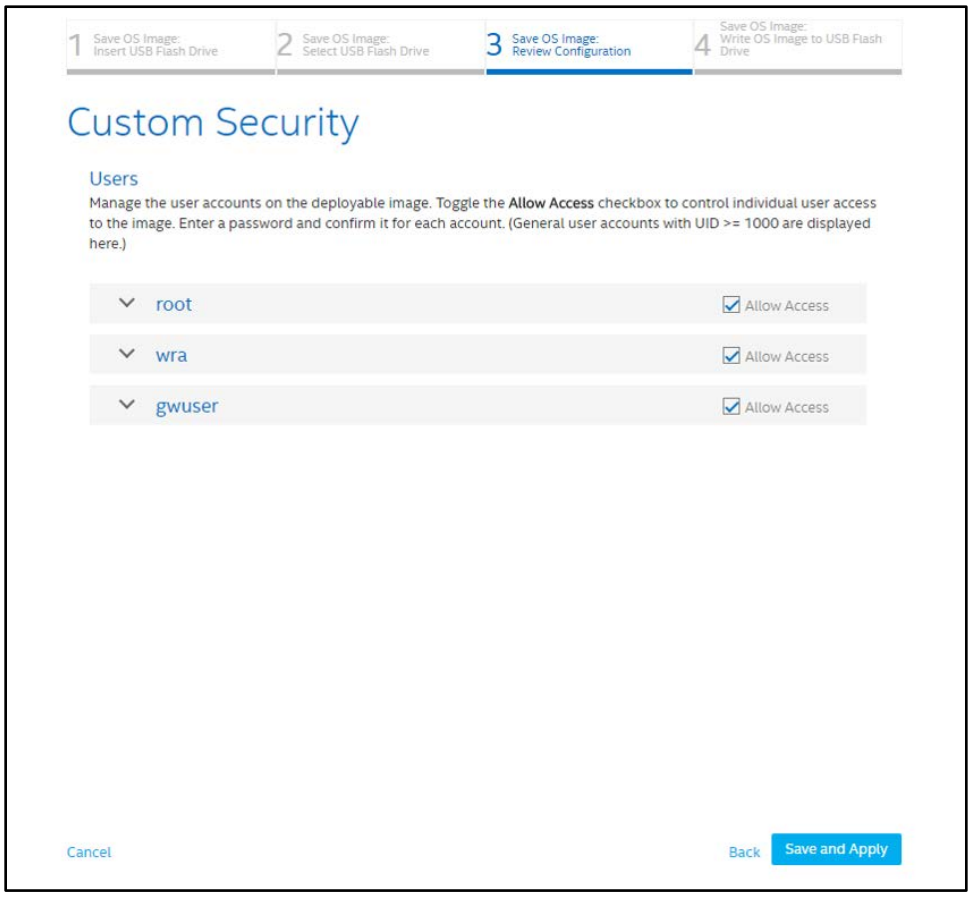


Click **Next**.

This Custom Security Users controls the specific users that are allowed access to the locked-down OS image. This page displays all of the users that are allowed access to the image.

Click the **Allow Access** toggle switch to control the access of the corresponding user. A checkmark indicates that the user has access.

Figure 11. Custom Security Page – Users



To change a user's password, click the dropdown next to the user's name.

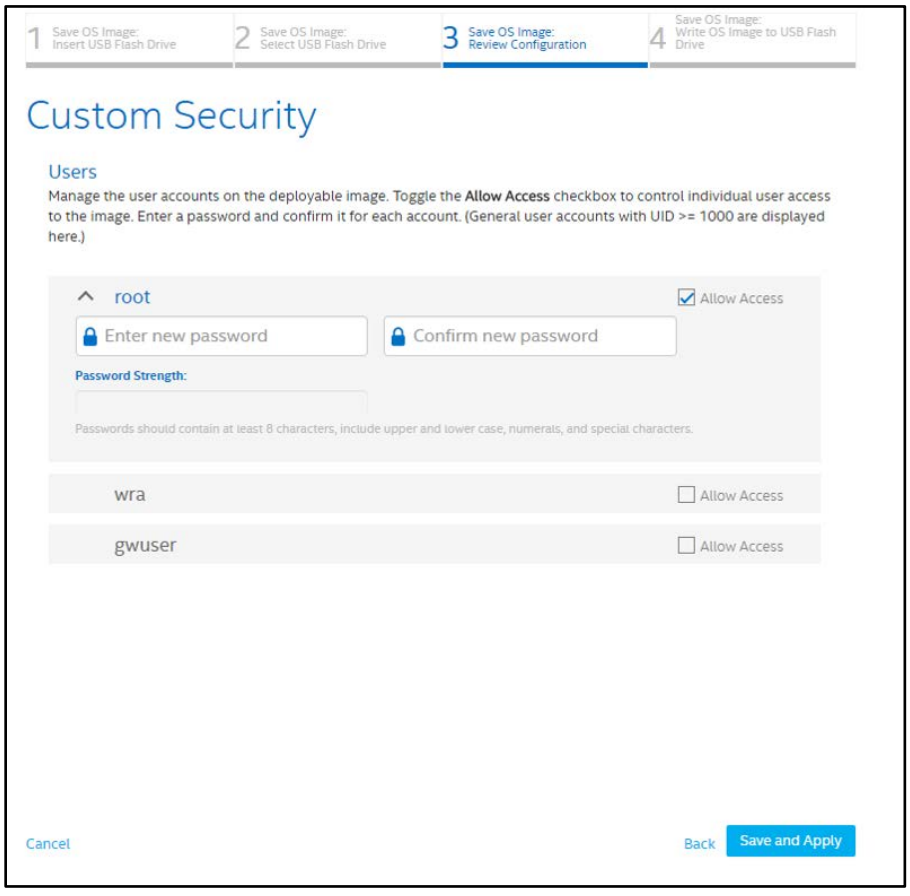
On the Custom Security Users screen you can create a new password for each user:

1. Type the new password into the **Enter new password** field
2. Retype the password in the **Confirm new password** field.

NOTE: The new password must be at least three characters long.

3. Click the **Allow Access** toggle switch to control the access of the corresponding user. A checkmark indicates that the user has access.

Figure 12. Custom Security Page – User Password Administration



Click **Save and Apply**. The locked-down OS image is saved.

2.2 Unsupported or Discontinued Features

The following features have been discontinued, or are no longer supported in this release.

- None

3 Fixed Issues

The table below contains the issues fixed in this release.

Table 1. Fixed Issues

Ref #	Description	Impact	Resolution
IDP3-1637	Unplugging and then plugging in the HDMI cable results in a crash when secure boot enabled.	This error was observed in the IDP XT 3.1.0.15 version.	Fixed
IDP3-1642	The Intel® IoT Gateway Developer Hub fails to create a USB image when using MI 3.1 GA + RCPL16 Pro update.	This error was observed in RCPL16.	Fixed
IDP3-1653	Deploying an image using the deploytool command to a Quark target takes longer than 1 hour.	This error was observed in RCPL16.	Fixed
MIPAP-580	The OS Package update fails when the network resets and checks for the connectivity by the Intel® IoT Gateway Developer Hub, resulting in the following error message: “Update Failed! Worker Process (working on another work) does not have the target result!”	This error was observed in RCPL16.	Fixed
MIPAP-595	When attempting to create a lockdown image, the following error may be encountered: “Error Saving OS Image”.	This error was observed when creating images from an RCPL16 upgrade.	Fixed

4 Known Issues and Errata

The table below contains the known issues and errata for this release.

Table 2. Known Issues and Errata

Ref #	Description	Workaround	Planned Fix
	Wind River® Helix App Cloud connectivity works only with a direct internet connection, not through a proxy server. The Helix App Cloud registration process will complete correctly but the agent will show 'offline', and will not function when behind a firewall.	Connect to the internet directly, outside of a firewall, without a proxy.	A fix is planned for a future release.
MIPAP-17	By default, the gateway boots in access point mode, with a default subnet of 192.168.1.0. This is a very common subnet for routers, and can cause conflicts.	Edit the `/etc/config/network` file or use the LuCI gateway configuration interface to change the default subnet. Go to **Network** > **Interfaces** > **LAN** > **Edit** > **IPv4 address**. Change the address, click **Save & Apply** then restart the system.	No fix is planned.
MIPAP-225	If a problem occurs during the process of deploying an OS to the gateway, later the gateway might boot from the USB drive but mount the gateway hard drive with the same UUID. `deploytool` will then be unable to run from the USB drive.	Delete the contents and partitions of the gateway hard drive, reboot to the USB drive, and re-run `deploytool` to deploy the gateway OS from the USB Drive to the gateway hard drive.	No fix is planned.
MIPAP-441	When the app cloud is launched, the following error message appears: "Error retrieving code from Helix App cloud".	Shut down the Intel® IoT Developer Hub and launch the app cloud again.	A fix is planned for a future release.
MIPAP-503	Using `deploytool` to deploy a new gateway from a USB flash drive image created with **Save OS Image** fails with "Failed to start McAfee Solidifier service" errors.	Manually copy `/boot/bzImage*idp` and `/boot/bzImage*idp.auth` from the USB flash drive to the gateway hard drive on `/media/sda1` as `bzImage` and `bzImage.auth` respectively.	A fix is planned for a future release.
MIPAP-515	**Upgrade to Pro** process will fail on Intel® Galileo™ Gen 2 systems with "Cannot allocate memory" error.	No workaround available. This is a known limitation with Galileo™ Gen 2, which occurs because it has only 256 MB of system memory.	No fix is planned.

Ref #	Description	Workaround	Planned Fix
MIPAP-541	The Intel® Developer Hub does not work properly (e.g., OS Update fails) after the Intel® IoT Developer Hub upgrades to a new version.	Clear the browser cache immediately after updating the OS.	A fix is planned for a future release.

MIPAP-559	Currently, there are 80 time zones available for use in the Gateway. The current version of Wind River Linux only contains 20 time zones. The discrepancy may hamper the ability of the cloud to communicate with the edge components. One of the time zones not included in the Wind River Linux is the Arizona Time Zone.	In general, it is not a good idea to depend on the time zone of the gateway. Most embedded system use Epoch time for communicating time with the cloud system. Epoch time is not dependent on time zone of the system.
		However, you can install additional time zone rpm's from the WinDistro repository. Here are the instructions for installing the Arizona Time Zone:
		`#smart channel --add windDistro type=rpm-md baseurl=https://distro.windriver.com/release/idp-3-xt/public_feeds/WR-IDP-3-XT-Intel-Baytrail-public-repo/RCPL13/all/`
		`#smart update`
		`#smart install tzdata-americas-2015g`
		`#export TZ=America/Phoenix`
		`#date`
			No fix is planned.

Ref #	Description	Workaround	Planned Fix
MIPAP-579	If you are using version 1.0.1, the Intel® IoT Developer Hub cannot be upgraded to latest version.	**Workaround 1** 1. Add the repo that has the latest Intel® IoT Developer Hub available. 2. Connect to the gateway using SSH or Serial Port so you can run commands on Intel® IoT Developer Hub. 3. Set up the network proxies if your network environment needs proxies. 4. Uninstall the Intel® IoT Developer Hub by running `smart remove -y iot-developer-hub` 5. Install the Intel® IoT Developer Hub by running `smart install -y iot-developer-hub` 6. Run `smart query --installed iot-developer-hub` to verify that the latest Intel® IoT Developer Hub version is installed. **Workaround 2** 1. Follow steps 1 - 3 in Workaround 1. 2. Run `echo "dummy" > /tmp/update-iot-dev-hub.sh` to create a dummy file. 3. Click the update button.	A fix is planned for a future release.
MIPAP-581	Sometimes all the OS packages are not completely updated when updating from RCPL13 GA to RCPL13 Respin. This occurs on Gateways working on a Quark platform.	Perform the OS package update process again until all the packages are updated.	No fix is planned.

MIPAP-593
MIPAP-597
	After running the process to fetch information for **Intel_Repository**, the following errors were noted:
	`error: Failed acquiring release file for 'Intel_Repository':`
	`error: https://download.01.org/iotgateway/rcpl13/i586/repodata/repomd.xml: server certificate verification failed. CAfile: /etc/ssl/certs/ca-certificates.crt CRLfile: none`
		Update the date manually using the following command:
		`root@WR-IDP-F3C9:~# date – s "DD MMM YYYY HH:MM:SS"`
			No fix is planned.

Ref #	Description	Workaround	Planned Fix
MIPAP-654	The Lockdown script may fail on the Quark platform: `deploytool -C -F -E -y -Y -d /media/sda1/usb.img --lockdown`	No workaround available.	A fix is planned for a future release.
MIPAP-655	OS upgrade process fails when attempting to move from RCPL13 to RCPL18. The following error message has been observed on Gateways running Quark: “The request got access denied: http status is 401!”	Follow these steps: 1. Connect to the Gateway using a command console, e.g. Putty. 2. Enter the command `systemctl status iot-dev-hub` 3. Observe the result and check if `smart upgrade -y` is running. 4. If `smart upgrade -y` is not running, then reboot your gateway; the OS Update process should be complete.	A fix is planned for a future release.
MIPAP-659	The Custom Save OS Image process throws an error on RCPL versions less than 18. `Unexpected error occurred. Try again. (Error code 32).`	No workaround available. The Custom Save OS Image is only supported on version WR7.0.0.18 or greater.	A fix is planned for a future release.

5 Wind River Linux 7 RCPL18 Changes

This section contains the changes in the Wind River Linux 7 operating system applicable to release 3.1.0.18.

```
LIN7-5789  Security Advisory - linux - CVE-2016-0821
LIN7-6121  Security Advisory - subversion - CVE-2016-2168
LIN7-6129  Security Advisory - wireshark - CVE-2016-4078
LIN7-6130  Security Advisory - libtasn1 - CVE-2016-4008
LIN7-6133  Security Advisory - Hostapd & wpa_supplicant - CVE-2016-4476
LIN7-6134  Security Advisory - wireshark - CVE-2016-4082
LIN7-6137  Security Advisory - wireshark - CVE-2016-4080
LIN7-6138  Security Advisory - subversion - CVE-2016-2167
LIN7-6140  Security Advisory - wireshark - CVE-2016-4418
LIN7-6146  Security Advisory - wireshark - CVE-2016-4081
LIN7-6147  Security Advisory - wpa_supplicant - CVE-2016-4477
LIN7-6150  Security Advisory - wireshark - CVE-2016-4421
LIN7-6189  Security Advisory - wireshark - CVE-2016-4417
LIN7-6192  Security Advisory - wireshark - CVE-2016-4085
LIN7-6193  Security Advisory - wireshark - CVE-2016-4079
LIN7-6198  Security Advisory - wireshark - CVE-2016-4006
LIN7-6270  Security Advisory - perl - CVE-2015-8853
LIN7-6278  Security Advisory - librsvg - CVE-2016-4348
LIN7-6296  Security Advisory - expat - CVE-2016-0718
LIN7-6305  Security Advisory - curl - CVE-2016-3739
LIN7-6323  Security Advisory - linux - CVE-2016-4485
LIN7-6326  Security Advisory - linux - CVE-2016-4581
LIN7-6335  Security Advisory - linux - CVE-2016-4580
LIN7-6348  Security Advisory - linux - CVE-2016-4805
LIN7-6385  Security Advisory - dosfstools - CVE-2016-4804
LIN7-6387  Security Advisory - imagemagick - CVE-2016-4563
LIN7-6393  Security Advisory - imagemagick - CVE-2016-4564
LIN7-6400  Security Advisory - glibc - CVE-2016-1234
LIN7-6409  Security Advisory - glibc - CVE-2016-3075
LIN7-6411  Security Advisory - glibc - CVE-2016-3706
LIN7-6414  Security Advisory - dosfstools - CVE-2015-8872
LIN7-6418  Security Advisory - imagemagick - CVE-2016-4562
LIN7-6419  Security Advisory - glibc - CVE-2016-4429
LIN7-6452  Security Advisory - qemu - CVE-2016-5338
LIN7-6456  Security Advisory - linux - CVE-2016-3707
LIN7-6458  Security Advisory - linux - CVE-2016-5829
LIN7-6459  Security Advisory - qemu - CVE-2016-2391
LIN7-6463  Security Advisory - qemu - CVE-2016-2392
LIN7-6466  Security Advisory - expat - CVE-2012-6702
LIN7-6467  Security Advisory - linux - CVE-2016-0758
LIN7-6470  Security Advisory - qemu - CVE-2016-2538
LIN7-6471  Security Advisory - expat - CVE-2016-5300
LIN7-6472  Security Advisory - qemu - CVE-2016-5337
LIN7-6473  Security Advisory - linux - CVE-2016-5828
LIN7-6474  Security Advisory - qemu - CVE-2016-5238
LIN7-6476  Security Advisory - linux - CVE-2014-9904
LIN7-6481  Security Advisory - linux - CVE-2016-3070
LIN7-6482  Security Advisory - linux - CVE-2016-3955
LIN7-6506  Security Advisory - wget - CVE-2016-4971
LIN7-6509  Security Advisory - xerces-c - CVE-2016-4463
LIN7-6528  Security Advisory - expat - CVE-2016-4472
LIN7-6535  Security Advisory - expat - CVE-2015-2716
LIN7-4926  rb_futex run failed on fsl-p10xx
LIN7-5924  Need to integrate gcc-4.9.2 0060-Only-allow-e500-double-in-
           SPE_SIMD_REGNO_P-registers.patch into wrlinux-7 gcc-4.9.1
LIN7-5943  igb Tx Unit Hangs on long scp transfers
LIN7-5984  Blacklisting GPLv3 ignored
```

LIN7-6100	Wind River Linux Kernel Command Line Tutorials, 7.0, document refers to destination directory, which does not exist.
LIN7-6232	Document that running Wind River Linux under Hyper-V is not supported.
LIN7-6263	wr-installer: An unhandled exception has occurred
LIN7-6378	powerpc-nf and ppc476-nf SDK toolchains on windows (mingw) may fail to load environment file
LIN7-6426	CLONE - [tz-announce] 2016e release of tz code and data available
LIN7-6443	Cannot recognize HSUART
LIN7-6451	MMC driver reports incorrect partition size at boot
LIN7-6489	CLONE - tz-announce] 2016f release of tz code and data available
LIN7-6492	iputils build fail with glibc-core
LIN7-6493	Zinq BSP: conflicts in spi_master.flag definitions
LIN7-6494	MD5 hash algorithm - Additional Information to reported security weaknesses
LIN7-6502	CLONE - Boot yocto initramfs core-image-minimal-initramfs failed
LIN7-6505	CLONE - wrl5 : netstat handle unresolvable IPv4 addresses better than for IPv6
LIN7-6532	tzcode-native_2016e.bb, do_fetch failed
LIN7-6536	Patch CVE-2016-3075.patch does not apply
LIN7-6613	kernel warnings on qemux86

6 How to Obtain this Release

6.1 Where to Find the Software

The Intel® IoT Gateway Developer Hub is integrated into the free download of the Intel® IoT Gateway Software Suite/Pro Software Suite which available at the Intel® IoT Platform Marketplace (IntelIotMarketplace.com)

NOTE: You must "Install OS Updates", restart the gateway, then "Upgrade to Pro" within the Intel® IoT Gateway Developer Hub to install and utilize the following Pro features:

- McAfee Embedded Control Pro features
- Save a security-hardened, deployable OS image to a USB flash drive
- Legally deploy the generated OS image onto other gateways for pilot or production deployments.

A license to upgrade to the Intel® IoT Gateway Pro Software Suite is also available for purchase on the Intel® IoT Platform Marketplace.

6.2 How to Install this Release

Instructions to install the Intel® IoT Gateway Software Suite OS image onto a compatible gateway and then access the Intel® IoT Gateway Developer Hub are included in the README file included in the Software Suite download.

Instructions are also included in the *Intel® IoT Gateway Technology: Gateway Installation Guide* in the chapter titled *Downloading and Installing the Gateway OS*. The document is available at https://software.intel.com/en-us/SetupGateway-hardware.

To get the latest release of the Intel® IoT Gateway Developer Hub software, go to the **Packages** page and click **Install Updates,** or click the update icon, if present.

7 Hardware and Software Compatibility

This chapter provides a summary of the hardware and software compatible with this release of the Intel® IoT Gateway Developer Hub.

7.1 Supported Web Browsers for the User Interface

The Intel® IoT Gateway Developer Hub user interface works best when accessed using one of these browsers:

- Microsoft Internet Explorer* 11
- Google Chrome* (version 49)
- Mozilla Firefox* (version 45)

7.2 Supported BIOS and Firmware

The Intel® IoT Gateway Developer Hub runs on top of the Wind River Linux 7 operating system with Wind River Intelligent Device Platform XT 3, which has the following BIOS requirements.

Table 3. BIOS Requirements

Gateway CPU	BIOS Requirement
Intel® Core™ processor	64-bit BIOS
Intel® Atom™ processor	64-bit BIOS
Intel® Quark™ processor	32-bit BIOS

7.3 Supported Gateway Hardware

The gateways listed below have been tested and qualified to work with Wind River Linux 7 operating system with Wind River Intelligent Device Platform XT 3.

Refer to the Gateway Comparison Tool web page (https://edc.intel.com/Gateway-Comparison) for the latest list of compatible gateways.

NOTE: The Intel® IoT Gateway Developer Hub interface works best on gateways based Intel® Atom™ or Core™ processors.

User interface performance is slow on Intel® Quark™ processor based gateways. Optimizations are planned for a future release. (See Known Issues and Errata)

7.3.1 Intel® Core™ Processor Gateways

- ADLink* MXE-5401
- Other gateways based on Intel® Core™ Processor 4000 Series

7.3.2 Intel® Atom™ Processor Gateways

- Advantech* Trek-572
- Advantech UTX-3115
- Axiomtek* ICO300-MI
- Dell Edge* Gateway 5000 Series
- Gigabyte* GB-BXBT-3825
- Gigabyte GB-TCV1
- Intel® NUC DE3815TYK
- Kontron* Kbox A-202
- Other gateways based on Intel® Atom™ Processor E3800 Series

7.3.3 Intel® Quark™ SoC Gateways

- Aaeon* AIOT-X1000
- BCM* BI255-1900J-IoT-DEV
- Kontron Kbox A-201
- SuperMicro* SYS-E100-8Q
- Intel® IoT Gateway DK200 Series
- Intel® IoT Gateway DK300 Series
- Intel® Galileo™ Gen 2
- Other gateways based on Intel® Quark™ SoC X1000 Series

NOTE: Due to slower processing times on the gateways based on Intel® Quark™ Gateways, it is best to use the Intel® IoT Developer Hub on a gateway with an Intel® Atom™ or Intel® Core™ processor.

7.4 Supported Sensors and Peripherals

This release of the Intel® IoT Developer Hub includes software support for the Omega RH-USB sensor and peripherals (http://www.omega.com/pptst/RH-USB.html). Other sensors and peripherals, and the software and drivers for them, may be added by the user.