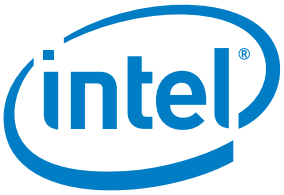


Intel® IoT Gateway Software Suite / Flex + Pro Software Suite Release Notes

Version 3.1.0.29 Production

Release Notes

November 2018

Document Number: 334680-010
Revision 3.1.0.29

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 that may cause the product to deviate from published specifications. Current characterized errata are available on request.

Copies of documents that 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
12 November 2018	3.1.0.29 Production Release	Added information on public key change for RCPL29.
31 October 2018	3.1.0.29 Production Release	Public Release of the latest version of the Intel® IoT Gateway Software Suite/Flex + Pro Software Suite, which includes Wind River Linux 7 RCPL fixed defects only.
29 May 2018	3.1.0.28 Production Release	Public Release of the latest version of the Intel® IoT Gateway Software Suite/Flex + Pro Software Suite, which includes Wind River Linux 7 RCPL updates
19 January 2018	3.1.0.27 Production Release	Public Release of the latest version of the Intel® IoT Gateway Software Suite/Flex + Pro Software Suite, which includes Wind River Linux 7 RCPL updates
18 September 2017	3.1.0.26 Production Release	Public Release of the latest version of the Intel® IoT Gateway Software Suite/Flex + Pro Software Suite, which includes Wind River Linux 7 RCPL updates
26 June 2017	3.1.0.25 Production Release	Public Release of the latest version of the Intel® IoT Gateway Software Suite/Flex + Pro Software Suite, which includes Wind River Linux 7 RCPL updates
27 March 2017	3.1.0.23 Production Release	Public Release of the latest version of the Intel® IoT Gateway Software Suite/Pro Software Suite, which includes Wind River Linux 7 RCPL updates.
9 January 2017	3.1.0.22 Production Release	Public Release of the latest version of the Intel® IoT Gateway Software Suite/Pro Software Suite, which includes Wind River Linux 7 RCPL updates.
14 November 2016	3.1.0.21 Production Release	Public Release of the latest version of the Intel® IoT Gateway Software Suite/Pro Software Suite, which includes security updates as well as general fixes and known issues. Beginning with version 3.1.0.21, the Developer Hub is not released for Quark platforms.
19 October 2016	3.1.0.20 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 several security updates, as well as general fixes and known issues.
19 September 2016	3.1.0.19 Production Release	Public Release of the latest version of the Intel® IoT Gateway Software Suite/Pro Software Suite, which includes the latest version of the Node-RED software available via the Intel® IoT Developer Hub, fixes to Wind River Intelligent Device Platform XT 3.1, and one security issue.

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.
18 April 2016	1.0.2 Production Release	Public Release of the Intel® IoT Developer Hub along with Wind River Intelligent Device Platform 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 specific to release 3.1.0.29 of the Intel® IoT Software Suite/Pro Software Suite, which includes the Intel® IoT Gateway Developer Hub. The document includes information about:

- Fixed issues
- Known errata
- Changes to Wind River* Linux 7
- How to get this release
- Compatible hardware and software

1.2 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 more efficient process controls. The Intel® IoT Gateway Software Suite/Pro Software Suite allows access to the Intel® IoT Gateway Developer Hub (see section 1.3).

Other features include:

Binary Runtime Images

- The Intel® IoT Gateway Software Suites are delivered as binary images. These binaries allow provide the features of the Software Suite and Pro Software Suite without recompiling a Linux OS image. This helps you get up and running in as little as 10 minutes.

Intel® IoT Gateway Software Suite

- Comes in two versions:
    - **Software Suite** is a pre-validated base binary image, with no ticketed support or development seats included. It includes the McAfee* Embedded Control Essential set of security tools.

- **Pro Software Suite** offers one year of ticketed support, Wind River development tools, and the McAfee Embedded Control Pro set of security tools.

1.3 About the Intel® IoT Gateway Developer Hub

The Intel® IoT Gateway Developer Hub is a web-based service that runs on the gateway. The Developer Hub gives you a hands-on sensor-to-cloud experience in a short time via the **Sensors** tab. It has built-in tutorials to teach you about tools like Node-RED* (a visual sensor-to-cloud programming interface) and the Wind River* Helix* App Cloud (a gateway application development environment hosted in the cloud) available from the **Documentation** tab.

Use one of these options to quickly connect sensors to the Intel® IoT Gateway Developer Hub and experience the fast sensor-to-cloud experience:

- Use the Omega* temperature & humidity sensor included in the Loaner Kit (a 6-month free loaner you can request from Demo Depot – for US, Canada, and EU). It contains a gateway and sensor to connect out of the box. You can use the Node Red* temperature flow out of the box. The Developer Hub has tutorials about adding humidity readings.
- Use any of the published recipes & packages (accessible via the hub) to evaluate additional sensors and cloud providers.

In addition, the Intel® IoT Developer Hub lets you add packages and develop package apps in the hub via the “Packages” tab. When you finish developing them, you can save a hardened OS image to a USB flash drive.

The Intel® IoT Gateway 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

- Add or remove online package repositories
- List installed packages
- Quickly add, update, or uninstall packages as needed

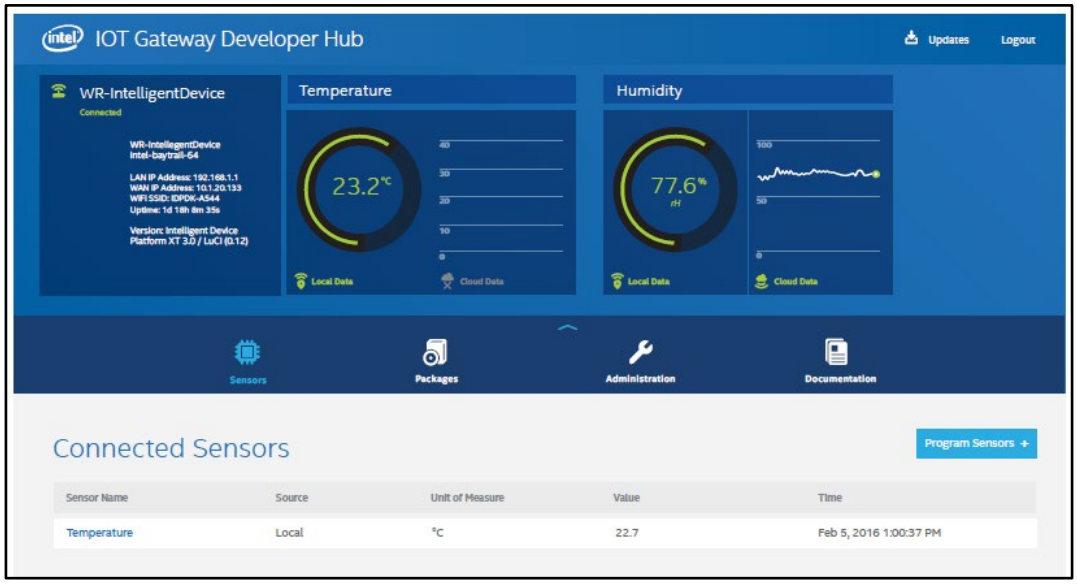
Gateway administration tools and resources

- 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*

Documentation

- One location to find tutorials and videos. Provides links to key online content.

Figure 1. The Intel® IoT Developer Hub User Interface



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

NOTE: You must **Upgrade to Pro** within the Developer Hub interface to use these 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 on other gateways for pilot or production deployments.

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

1.4 Intended Audience

This document is for all users of the Intel® IoT Gateway Software Suite / Pro Software Suite.

1.5 Related Documents

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

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

1.6 Technical Support

Free technical support is available from 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

This document uses these conventions:

- "Developer Hub" or "Dev Hub" refers to the Intel® IoT Developer Hub.
- "Gateway" and "IoT Gateway" refers to any qualified Intel® IoT Gateway device.
- `This font` is for code examples, command line entries, API names, parameters, filenames, directory paths, and executables.
- **Bold text** is for graphical user interface entries and buttons.

2 Features in This Release

This chapter describes the new, changed, and unchanged elements particular to this release.

2.1 New Features

This is a maintenance release. There are no new features.

2.2 Unsupported or Discontinued Features

- Wind River* Helix* Device Cloud (HDC)
- Helix* App Cloud (HAC)

3 Security Updates

This section contains information regarding the security updates. Additional information is in Fixed Issues and Wind River Linux 7 RCPL28 Changes.

3.1 McAfee Security Updates

The Intel® IoT Gateway Software Suite contains the McAfee Embedded Control Essentials version 6.6.2.126.

An upgrade to Intel® IoT Gateway Pro Software Suite includes an upgrade to McAfee Embedded Control Pro version 6.6.4.110. For information about this version, see: http://www.mcafee.com/us/products/embedded-control.aspx

3.2 Wind River Security Updates

Wind River analyzes industry-wide security alerts and incorporates them into the Wind River Linux 7 RCPL releases.

For documentation about specific Wind River security issues:

1. Go to https://knowledge.windriver.com/en-us/Wind_River_Support_Network.
2. Click the **Wind River Support Network** drop-down list in the left corner.
3. Select **Products.**
4. Select **Linux** under **Operating Systems.**
5. Select **Security Notices** under **Linux 7.**
6. Select **Downloads/Security Notices.**
7. Select the most recent document to download.

4 Fixed Issues

Defect ID	Summary
LIN7-10000	Security Advisory - mercurial - CVE-2018-13347
LIN7-10001	Security Advisory - nagios-core - CVE-2018-13441
LIN7-10002	Security Advisory - mercurial - CVE-2018-13348
LIN7-10012	Security Advisory - znc - CVE-2018-14056
LIN7-10019	Security Advisory - linux - CVE-2018-5390
LIN7-10022	Security Advisory - linux - CVE-2018-14617
LIN7-10025	Security Advisory - mutt - CVE-2018-14357
LIN7-10030	Security Advisory - wireshark - CVE-2018-14339
LIN7-10035	Security Advisory - linux - CVE-2018-9422
LIN7-10036	Security Advisory - mutt - CVE-2018-14354
LIN7-10039	Security Advisory - mutt - CVE-2018-14355
LIN7-10040	Security Advisory - ffmpeg - CVE-2018-14394
LIN7-10041	Security Advisory - mutt - CVE-2018-14349
LIN7-10044	Security Advisory - imagemagick - CVE-2018-14437
LIN7-10048	Security Advisory - mutt - CVE-2018-14358
LIN7-10049	Security Advisory - libxdmcp - CVE-2017-2625
LIN7-10050	Security Advisory - mysql - CVE-2018-3070
LIN7-10051	Security Advisory - mysql - CVE-2018-3081
LIN7-10054	Security Advisory - mutt - CVE-2018-14353
LIN7-10055	Security Advisory - mutt - CVE-2018-14356
LIN7-10056	Security Advisory - util-linux - CVE-2017-2616
LIN7-10061	Security Advisory - mysql - CVE-2018-3066
LIN7-10063	Security Advisory - wireshark - CVE-2018-14340
LIN7-10066	Security Advisory - spice - CVE-2016-9577
LIN7-10067	Security Advisory - busybox - CVE-2015-9261
LIN7-10068	Security Advisory - imagemagick - CVE-2018-14551
LIN7-10070	Security Advisory - spice - CVE-2016-9578
LIN7-10071	Security Advisory - ffmpeg - CVE-2018-14395
LIN7-10072	Security Advisory - ffmpeg - CVE-2018-1999012
LIN7-10073	Security Advisory - wireshark - CVE-2018-14343
LIN7-10075	Security Advisory - mutt - CVE-2018-14351
LIN7-10080	Security Advisory - imagemagick - CVE-2018-14434

LIN7-10081 Security Advisory - wireshark - CVE-2018-14368
LIN7-10083 Security Advisory - wireshark - CVE-2018-14369
LIN7-10084 Security Advisory - xorg-x11-server - CVE-2017-2624
LIN7-10085 Security Advisory - libxml2 - CVE-2018-14404
LIN7-10086 Security Advisory - fuse - CVE-2018-10906
LIN7-10087 Security Advisory - mutt - CVE-2018-14359
LIN7-10092 Security Advisory - bind - CVE-2017-3145
LIN7-10095 Security Advisory - imagemagick - CVE-2018-14435
LIN7-10097 Security Advisory - linux - CVE-2017-18344
LIN7-10099 Security Advisory - mutt - CVE-2018-14352
LIN7-10105 Security Advisory - mutt - CVE-2018-14350
LIN7-10106 Security Advisory - libice - CVE-2017-2626
LIN7-10108 Security Advisory - mysql - CVE-2018-2767
LIN7-10109 Security Advisory - mysql - CVE-2018-3058
LIN7-10110 Security Advisory - wireshark - CVE-2018-14341
LIN7-10111 Security Advisory - imagemagick - CVE-2018-14436
LIN7-10114 Security Advisory - linux - CVE-2018-14734
LIN7-10115 Security Advisory - mutt - CVE-2018-14362
LIN7-10116 Security Advisory - ffmpeg - CVE-2018-1999010
LIN7-10117 Security Advisory - mysql - CVE-2018-3063
LIN7-10126 Security Advisory - libxml2 - CVE-2018-14567
LIN7-10127 Security Advisory - ceph - CVE-2016-9579
LIN7-10133 Security Advisory - wpa-supplicant - CVE-2018-14526
LIN7-10135 Security Advisory - ceph - CVE-2016-8626
LIN7-10137 Security Advisory - libxcursor - CVE-2015-9262
LIN7-10140 Security Advisory - dracut - CVE-2016-8637
LIN7-10145 Security Advisory - libcgroup - CVE-2018-14348
LIN7-10149 Security Advisory - php - CVE-2018-14851
LIN7-10150 Security Advisory - php - CVE-2018-14883
LIN7-2118 Security Advisory - linux - CVE-2014-8481
LIN7-2687 Security Advisory - ffmpeg & libav - CVE-2011-4352
LIN7-6274 Security Advisory - quagga - CVE-2016-4049
LIN7-6526 Security Advisory - bind - CVE-2016-6170
LIN7-6934 Security Advisory - linux - CVE-2016-7042
LIN7-7262 Security Advisory - linux - CVE-2016-6213
LIN7-7586 Security Advisory - shadow - CVE-2016-6252
LIN7-8123 Security Advisory - libxml2 - CVE-2017-8872
LIN7-8440 Security Advisory - libtiff - CVE-2017-11613

LIN7-8832 Security Advisory - wpa_supplicant - CVE-2015-0210
LIN7-8915 Security Advisory - libarchive - CVE-2017-14503
LIN7-8932 Security Advisory - libvorbis - CVE-2017-14160
LIN7-8939 Security Advisory - libarchive - CVE-2017-14501
LIN7-9162 Security Advisory - linux - CVE-2017-16538
LIN7-9248 Security Advisory - libtiff - CVE-2017-17095
LIN7-9271 Security Advisory - linux - CVE-2017-1000410
LIN7-9308 Security Advisory - linux - CVE-2017-17807
LIN7-9344 Security Advisory - linux - CVE-2017-5715 - Spectre Attack
LIN7-9360 Security Advisory - linux - CVE-2018-5333
LIN7-9386 Security Advisory - linux - CVE-2018-5344
LIN7-9416 Security Advisory - php - CVE-2018-5712
LIN7-9429 Security Advisory - libgd&php - CVE-2018-5711
LIN7-9441 Security Advisory - libtiff - CVE-2018-5784
LIN7-9445 Security Advisory - linux - CVE-2017-18079
LIN7-9450 Security Advisory - linux - CVE-2018-1000004
LIN7-9453 Security Advisory - linux - CVE-2018-5750
LIN7-9469 Security Advisory - libxml2 - CVE-2017-5130
LIN7-9472 Security Advisory - libxml2 - CVE-2017-7376
LIN7-9476 Security Advisory - wireshark - CVE-2018-7418
LIN7-9477 Security Advisory - linux - CVE-2018-6927
LIN7-9480 Security Advisory - binutils - CVE-2018-7208
LIN7-9481 Security Advisory - librsvg - CVE-2018-1000041
LIN7-9482 Security Advisory - systemd - CVE-2018-1049
LIN7-9484 Security Advisory - glibc - CVE-2018-6485
LIN7-9486 Security Advisory - libtiff - CVE-2018-7456
LIN7-9488 Security Advisory - quagga - CVE-2018-5378
LIN7-9489 Security Advisory - wpa_supplicant - CVE-2015-5315
LIN7-9490 Security Advisory - imagemagick - CVE-2018-7470
LIN7-9491 Security Advisory - cups - CVE-2017-18190
LIN7-9492 Security Advisory - ntp - CVE-2018-7185
LIN7-9494 Security Advisory - shadow - CVE-2018-7169
LIN7-9495 Security Advisory - wireshark - CVE-2018-7334
LIN7-9496 Security Advisory - libid3tag - CVE-2004-2779
LIN7-9497 Security Advisory - glibc - CVE-2018-1000001
LIN7-9501 Security Advisory - glibc - CVE-2018-6551
LIN7-9502 Security Advisory - qemu - CVE-2017-18043
LIN7-9503 Security Advisory - imagemagick - CVE-2018-6405

LIN7-9504 Security Advisory - patch - CVE-2018-6951
LIN7-9505 Security Advisory - binutils - CVE-2018-6759
LIN7-9507 Security Advisory - wireshark - CVE-2018-7323
LIN7-9508 Security Advisory - linux - CVE-2017-16911
LIN7-9509 Security Advisory - php - CVE-2015-9253
LIN7-9515 Security Advisory - libxml2 - CVE-2017-7375
LIN7-9520 Security Advisory - wireshark - CVE-2018-7421
LIN7-9523 Security Advisory - wireshark - CVE-2018-7324
LIN7-9526 Security Advisory - quagga - CVE-2018-5379
LIN7-9527 Security Advisory - quagga - CVE-2018-5381
LIN7-9531 Security Advisory - linux - CVE-2018-7492
LIN7-9533 Security Advisory - wireshark - CVE-2018-7417
LIN7-9535 Security Advisory - binutils - CVE-2018-6543
LIN7-9539 Security Advisory - ntp - CVE-2018-7170
LIN7-9540 Security Advisory - wireshark - CVE-2018-7320
LIN7-9544 Security Advisory - unzip - CVE-2018-1000035
LIN7-9546 Security Advisory - ntp - CVE-2018-7184
LIN7-9547 Security Advisory - wireshark - CVE-2018-7322
LIN7-9549 Security Advisory - linux - CVE-2017-16914
LIN7-9550 Security Advisory - ntp - CVE-2018-7182
LIN7-9553 Security Advisory - python - CVE-2018-1000030
LIN7-9556 Security Advisory - quagga - CVE-2018-5380
LIN7-9557 Security Advisory - patch - CVE-2018-6952
LIN7-9558 Security Advisory - wireshark - CVE-2018-7336
LIN7-9559 Security Advisory - imagemagick - CVE-2018-7443
LIN7-9562 Security Advisory - wireshark - CVE-2018-7332
LIN7-9563 Security Advisory - patch - CVE-2016-10713
LIN7-9565 Security Advisory - hostapd - CVE-2015-5314
LIN7-9566 Security Advisory - ntp - CVE-2018-7183
LIN7-9567 Security Advisory - php - CVE-2016-10712
LIN7-9576 Security Advisory - linux - CVE-2017-18203
LIN7-9577 Security Advisory - linux - CVE-2017-18208
LIN7-9580 Security Advisory - libtiff - CVE-2014-8130
LIN7-9581 Security Advisory - binutils - CVE-2018-7568
LIN7-9582 Security Advisory - memcached - CVE-2018-1000115
LIN7-9584 Security Advisory - mercurial - CVE-2018-1000132
LIN7-9585 Security Advisory - krb5 - CVE-2018-5729
LIN7-9589 Security Advisory - binutils - CVE-2018-7642

LIN7-9590 Security Advisory - imagemagick - CVE-2017-18209
LIN7-9591 Security Advisory - samba - CVE-2018-1050
LIN7-9592 Security Advisory - samba - CVE-2018-1057
LIN7-9593 Security Advisory - linux - CVE-2017-18216
LIN7-9594 Security Advisory - linux - CVE-2017-18204
LIN7-9597 Security Advisory - linux - CVE-2018-1066
LIN7-9599 Security Advisory - linux - CVE-2017-18221
LIN7-9603 Security Advisory - linux - CVE-2017-18232
LIN7-9604 Security Advisory - binutils - CVE-2018-7570
LIN7-9605 Security Advisory - curl - CVE-2018-1000120
LIN7-9606 Security Advisory - qemu - CVE-2018-7550
LIN7-9608 Security Advisory - php - CVE-2018-7584
LIN7-9609 Security Advisory - xerces-c - CVE-2017-12627
LIN7-9610 Security Advisory - curl - CVE-2018-1000122
LIN7-9611 Security Advisory - linux - CVE-2018-7995
LIN7-9612 Security Advisory - memcached - CVE-2018-1000127
LIN7-9613 Security Advisory - linux - CVE-2018-7740
LIN7-9615 Security Advisory - krb5 - CVE-2018-5730
LIN7-9620 Security Advisory - linux - CVE-2018-7755
LIN7-9622 Security Advisory - binutils - CVE-2018-7643
LIN7-9623 Security Advisory - linux - CVE-2018-7757
LIN7-9624 Security Advisory - net-snmp - CVE-2018-1000116
LIN7-9625 Security Advisory - strongswan - CVE-2017-11185
LIN7-9626 Security Advisory - curl - CVE-2018-1000121
LIN7-9634 Security Advisory - imagemagick - CVE-2018-9135
LIN7-9635 Security Advisory - libtiff - CVE-2018-8905
LIN7-9636 Security Advisory - imagemagick - CVE-2018-8960
LIN7-9638 Security Advisory - linux - CVE-2018-1092
LIN7-9639 Security Advisory - linux - CVE-2018-7566
LIN7-9641 Security Advisory - apache - CVE-2017-15710
LIN7-9642 Security Advisory - cups - CVE-2017-18248
LIN7-9647 Security Advisory - linux - CVE-2018-1093
LIN7-9648 Security Advisory - imagemagick - CVE-2018-9133
LIN7-9650 Security Advisory - imagemagick - CVE-2017-18252
LIN7-9651 Security Advisory - imagemagick - CVE-2017-18251
LIN7-9652 Security Advisory - imagemagick - CVE-2017-18254
LIN7-9653 Security Advisory - imagemagick - CVE-2018-8804
LIN7-9654 Security Advisory - apache - CVE-2018-1303

LIN7-9655 Security Advisory - apache - CVE-2017-15715
LIN7-9659 Security Advisory - nasm - CVE-2018-8883
LIN7-9660 Security Advisory - linux - CVE-2017-18255
LIN7-9661 Security Advisory - linux - CVE-2018-1068
LIN7-9663 Security Advisory - nasm - CVE-2018-8881
LIN7-9664 Security Advisory - linux - CVE-2018-1094
LIN7-9665 Security Advisory - apache - CVE-2018-1283
LIN7-9666 Security Advisory - linux - CVE-2017-18249
LIN7-9667 Security Advisory - nasm - CVE-2018-8882
LIN7-9668 Security Advisory - libvirt - CVE-2018-1064
LIN7-9670 Security Advisory - linux - CVE-2018-8822
LIN7-9673 Security Advisory - apache - CVE-2018-1312
LIN7-9679 Security Advisory - patch - CVE-2018-1000156
LIN7-9684 Security Advisory - linux - CVE-2018-10021
LIN7-9685 Security Advisory - wireshark - CVE-2018-9259
LIN7-9687 Security Advisory - libxml2 - CVE-2017-18258
LIN7-9689 Security Advisory - wireshark - CVE-2018-9256
LIN7-9692 Security Advisory - wireshark - CVE-2018-9267
LIN7-9697 Security Advisory - ruby - CVE-2018-8779
LIN7-9698 Security Advisory - libxml2 - CVE-2018-9251
LIN7-9699 Security Advisory - wireshark - CVE-2018-9262
LIN7-9700 Security Advisory - ruby - CVE-2017-17742
LIN7-9704 Security Advisory - wireshark - CVE-2018-9265
LIN7-9705 Security Advisory - corosync - CVE-2018-1084
LIN7-9707 Security Advisory - wireshark - CVE-2018-9272
LIN7-9708 Security Advisory - wireshark - CVE-2018-9269
LIN7-9710 Security Advisory - wireshark - CVE-2018-9261
LIN7-9711 Security Advisory - ruby - CVE-2018-8780
LIN7-9713 Security Advisory - wireshark - CVE-2018-9258
LIN7-9714 Security Advisory - wireshark - CVE-2018-9263
LIN7-9715 Security Advisory - ruby - CVE-2018-8778
LIN7-9716 Security Advisory - wireshark - CVE-2018-9260
LIN7-9717 Security Advisory - wireshark - CVE-2018-9270
LIN7-9719 Security Advisory - ruby - CVE-2018-8777
LIN7-9720 Security Advisory - wireshark - CVE-2018-9268
LIN7-9724 Security Advisory - mysql - CVE-2018-2781
LIN7-9726 Security Advisory - mysql - CVE-2018-2813
LIN7-9728 Security Advisory - linux - CVE-2018-10087

LIN7-9730 Security Advisory - mysql - CVE-2018-2817
LIN7-9731 Security Advisory - postfix - CVE-2017-10140
LIN7-9732 Security Advisory - libvorbis - CVE-2018-10392
LIN7-9734 Security Advisory - ghostscript - CVE-2018-10194
LIN7-9736 Security Advisory - mysql - CVE-2018-2819
LIN7-9737 Security Advisory - ghostscript - CVE-2016-9601
LIN7-9741 Security Advisory - mysql - CVE-2018-2761
LIN7-9746 Security Advisory - php - CVE-2018-10547
LIN7-9748 Security Advisory - php - CVE-2018-10545
LIN7-9750 Security Advisory - php - CVE-2018-10546
LIN7-9752 Security Advisory - mysql - CVE-2018-2773
LIN7-9754 Security Advisory - mysql - CVE-2018-2771
LIN7-9755 Security Advisory - openssl - CVE-2018-0737
LIN7-9757 Security Advisory - imagemagick - CVE-2018-10177
LIN7-9765 Security Advisory - mysql - CVE-2018-2755
LIN7-9767 Security Advisory - mysql - CVE-2018-2818
LIN7-9775 Security Advisory - gunicorn - CVE-2018-1000164
LIN7-9776 Security Advisory - linux - CVE-2018-10124
LIN7-9777 Security Advisory - php - CVE-2018-10548
LIN7-9778 Security Advisory - libvorbis - CVE-2018-10393
LIN7-9779 Security Advisory - php - CVE-2018-10549
LIN7-9781 Security Advisory - perl - CVE-2018-6913
LIN7-9786 Security Advisory - libsoup - CVE-2017-2885
LIN7-9789 Security Advisory - flac - CVE-2017-6888
LIN7-9790 Security Advisory - linux - CVE-2018-8781
LIN7-9791 Security Advisory - linux - CVE-2018-1087
LIN7-9792 Security Advisory - linux - CVE-2018-8897
LIN7-9796 Security Advisory - linux - CVE-2018-10675
LIN7-9804 Security Advisory - blktrace - CVE-2018-10689
LIN7-9808 Security Advisory - imagemagick - CVE-2018-10804
LIN7-9809 Security Advisory - phpmyadmin - CVE-2017-18264
LIN7-9813 Security Advisory - ncurses - CVE-2018-10754
LIN7-9815 Security Advisory - linux - CVE-2018-10940
LIN7-9817 Security Advisory - xdg-utils - CVE-2017-18266
LIN7-9818 Security Advisory - wget - CVE-2018-0494
LIN7-9819 Security Advisory - linux - CVE-2018-1130
LIN7-9820 Security Advisory - libtiff - CVE-2018-10963
LIN7-9828 Security Advisory - procps - CVE-2018-1122

LIN7-9829 Security Advisory - procps - CVE-2018-1123
LIN7-9830 Security Advisory - procps - CVE-2018-1124
LIN7-9831 Security Advisory - procps - CVE-2018-1125
LIN7-9832 Security Advisory - procps - CVE-2018-1126
LIN7-9838 Security Advisory - imagemagick - CVE-2017-18273
LIN7-9841 Security Advisory - curl - CVE-2018-1000300
LIN7-9846 Security Advisory - libvorbis - CVE-2018-5146
LIN7-9848 Security Advisory - linux - CVE-2018-1000199
LIN7-9850 Security Advisory - sudo - CVE-2016-7076
LIN7-9851 Security Advisory - imagemagick - CVE-2018-11251
LIN7-9853 Security Advisory - glibc - CVE-2018-11236
LIN7-9858 Security Advisory - curl - CVE-2018-1000301
LIN7-9859 Security Advisory - imagemagick - CVE-2017-18271
LIN7-9864 Security Advisory - git - CVE-2018-11235
LIN7-9865 Security Advisory - qemu - CVE-2015-5745
LIN7-9869 Security Advisory - qemu - CVE-2015-5278
LIN7-9871 Security Advisory - file - CVE-2018-10360
LIN7-9873 Security Advisory - strongswan - CVE-2018-5388
LIN7-9874 Security Advisory - mdadm - CVE-2014-5220
LIN7-9875 Security Advisory - ghostscript - CVE-2018-11645
LIN7-9876 Security Advisory - libgcrypt - CVE-2018-0495
LIN7-9879 Security Advisory - openssl - CVE-2018-0732
LIN7-9883 Security Advisory - gnupg - CVE-2018-12020
LIN7-9884 Security Advisory - perl - CVE-2018-12015
LIN7-9886 Security Advisory - imagemagick - CVE-2018-11655
LIN7-9887 Security Advisory - imagemagick - CVE-2018-11656
LIN7-9889 Security Advisory - linux - CVE-2018-12233
LIN7-9890 Security Advisory - imagemagick - CVE-2018-11625
LIN7-9892 Security Advisory - qemu - CVE-2018-11806
LIN7-9897 Security Advisory - linux - CVE-2017-7518
LIN7-9903 Security Advisory - linux - CVE-2017-7482
LIN7-9906 Security Advisory - ntp - CVE-2018-12327
LIN7-9910 Security Advisory - strongswan - CVE-2018-10811
LIN7-9912 Security Advisory - qemu - CVE-2016-9603
LIN7-9915 Security Advisory - linux - CVE-2018-10853
LIN7-9918 Security Advisory - linux - CVE-2017-0861
LIN7-9922 Security Advisory - qemu - CVE-2017-2620
LIN7-9924 Security Advisory - python - CVE-2018-1061

LIN7-9926 Security Advisory - php - CVE-2018-12882
LIN7-9933 Security Advisory - imagemagick - CVE-2018-12599
LIN7-9936 Security Advisory - qemu - CVE-2017-7493
LIN7-9942 Security Advisory - imagemagick - CVE-2018-12600
LIN7-9944 Security Advisory - linux - CVE-2018-1000204
LIN7-9946 Security Advisory - linux - CVE-2017-0786
LIN7-9947 Security Advisory - qemu - CVE-2018-12617
LIN7-9950 Security Advisory - qemu - CVE-2017-15119
LIN7-9958 Security Advisory - ffmpeg - CVE-2018-12458
LIN7-9959 Security Advisory - bind - CVE-2018-5738
LIN7-9960 Security Advisory - linux - CVE-2018-13405
LIN7-9962 Security Advisory - ceph - CVE-2018-1129
LIN7-9970 Security Advisory - dhcp - CVE-2018-5732
LIN7-9971 Security Advisory - nagios-core - CVE-2018-13457
LIN7-9974 Security Advisory - libsoup - CVE-2018-12910
LIN7-9976 Security Advisory - linux - CVE-2018-13406
LIN7-9981 Security Advisory - znc - CVE-2018-14055
LIN7-9982 Security Advisory - imagemagick - CVE-2018-13153
LIN7-9989 Security Advisory - minicom - CVE-2017-7467
LIN7-9990 Security Advisory - mercurial - CVE-2018-13346
LIN7-9996 Security Advisory - nagios-core - CVE-2018-13458
LIN7-9998 Security Advisory - dhcp - CVE-2018-5733
LIN7-10014 CLONE - Update Intel microcode version 20180703
LIN7-10016 WARNING: at kernel/time/clockevents.c:241 clockevents_program_event+0x14c/0x15c
LIN7-10148 CLONE - Update Intel microcode version 20180807
LIN7-10156 wr7 can not enter rootfs
LIN7-4292 Cannot open shared object file:libdevmapper-event-lvm2snapshot.so:
LIN7-8118 Backporting patch to fix glibc 2.24 and RTLD_NEXT issues
LIN7-9173 process crash in glibc
LIN7-9400 The default init manager of glibc-core is sysvinit?
LIN7-9570 API change declared in release
LIN7-9571 Update microcode version 20180312
LIN7-9631 CLONE - [tz-announce] 2018d release of tz code and data available
LIN7-9681 meltdown/spectre: check upstream qemu patches
LIN7-9682 qemux86: Timed out waiting for device dev-ttyS0.devicex86
LIN7-9683 fail to connect qemu VM client with VNC .
LIN7-9721 qemux86: Failed to start Journal Service

LIN7-9722	Can't find releasemap file of LB21_7.0_RCPL0029
LIN7-9797	fsl-ls10xx BSP is categorized in PPC family in Getting Started
LIN7-9798	CLONE - [tz-announce] 2018e release of tz code and data available
LIN7-9801	All builds of pseudo fail
LIN7-9834	Update Intel microcode version 20180425

5 Issues and Errata

The table below contains the known issues and errata for this release. For further details on utilizing the Intel® IoT Gateway Developer Hub and workarounds, see the Intel® IoT Gateway Technology: Troubleshooting Guide available from the Development Hub interface.

NOTE: Beginning with version 3.1.0.21, the Developer Hub is not available for Intel® Quark™ platforms. Issues relating to Intel® Quark™ platforms will not be resolved.

Table 1. Known Issues and Errata

Ref #	Description	Workaround
	Wind River* Helix App Cloud connectivity works only with a direct internet connection, not through a proxy server. The Helix App Cloud registration process completes, but the agent shows 'offline', and does not work behind a firewall.	Connect to the internet directly, outside of a firewall, without a proxy.
MIPAP-17	By default, the gateway boots in access point mode, with a default subnet of 192.168.1.0. This is a 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: 1. Go to **Network** > **Interfaces** > **LAN** > **Edit** > **IPv4 address** 2. Change the address 3. Click **Save & Apply** 4. Restart the system.
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.

Ref #	Description	Workaround
MIPAP-669	While attempting to register the Gateway on the Helix App Cloud, the connection is lost, and a message displays: `Server Connection Lost. Please reload the page`	Try to connect with the cloud and register the Gateway later. To connect to the Helix App Cloud and register the Gateway: 1. Start the Gateway and log in. 2. Connect a PC to the Gateway. 3. Open the Gateway in a browser. 4. Click the **Administration** link on the IoT Developer Hub Interface (see Figure 1). 5. Click the **App Cloud Launch** link. 6. Select the **Unique ID** and copy it to the clipboard. 7. Click **Continue to Helix App Cloud**. 8. Click **Register Now** and follow the instructions. 9. Log into the Helix App Cloud using your new credentials. 10. Click **New Device**. 11. Click **Register an existing device using its unique ID**. 12. Paste the **Unique ID** you copied in step 6 and click **Next**. 13. Click **Register Device**.
MIPAP-691	While clicking the **Launch** App Cloud in the **Administration** tab, an error message results: `Error retrieving code from Helix App Cloud`	None

6 Wind River Linux 7 RCPL29 Changes

This is a maintenance release. There are no new features, only defect fixes.

6.1 How to Update the Public Key

To update the RCPL29 public key, proceed as follows:

1. Update smart channels.
2. Load the new key:

   ```
   # smart download ess-pbk;rpm -ivh ess-pbk*.rpm
   ```

3. Upgrade the Quark system.

6.2 How to Upgrade the Security Flash

After upgrading the Quark system to RCPL29, upgrade the security flash.

1. Access the target console.
2. From the console, enter the following command:

   ```
   # capsule_update -n Flash-crosshill-8M-secure.cap
   ```

   Note:
   You can update the flash with the **DediProg** tool directly using the **Flash-crosshill-8M-secure.bin** file.

7 How to Get Release 3.1.0.29

7.1 Where to Get the Software

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

NOTE: Use “Install OS Updates”, restart the gateway, then “Upgrade to Pro” within the Developer Hub interface to install and use these 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 on other gateways for pilot or production deployments.

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

7.2 How to Install this Release

Instructions to install the Intel® IoT Gateway Software Suite OS image on 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 Developer Hub software, go to the **Packages** page and click **Install Updates,** or click the update icon, if present, for the IoT Developer Hub.

8 Hardware and Software Compatibility

NOTE: Beginning with version 3.1.0.21, the Developer Hub is not released for Intel® Quark™ platforms.

8.1 Supported Web Browsers for the User Interface

The Developer Hub interface works best with these browsers:

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

8.2 Supported BIOS and Firmware

The Developer Hub runs on the Wind River Linux 7 operating system with Wind River Intelligent Device Platform XT 3. BIOS requirements depend on the gateway processor:

Table 2. BIOS Requirements

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

8.3 Supported Gateway Hardware

The gateways below work with Wind River Linux 7 operating system with Wind River Intelligent Device Platform XT 3.

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

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

8.3.1 Intel® Core™ Processor Gateways

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

8.3.2 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 (code named Thin Canyon)
- Kontron* Kbox A-202
- Other gateways based on Intel Atom® Processor E3800 Series

8.4 Supported Sensors and Peripherals

This release of the Intel® IoT Gateway Developer Hub includes software support for the Omega RH-USB sensor and peripherals (http://www.omega.com/pptst/RH-USB.html). You can add other sensors and peripherals, and the software and drivers for the sensors and peripherals.