Security & Safety

IGEL Product Security Information

Here you find all IGEL Security Notices (ISN). They inform you of any major vulnerabilities that have been found in IGEL software products and of how to fix or mitigate these.

Besides that, most IGEL software updates fix several minor vulnerabilities. You find information about these in the Release Notes that are published with each release.

Security Announcements Mailing List
To get new ISNs and ISN updates delivered to your inbox, subscribe to the Security Announcements Mailing List. Go to igel.com[1] and find the "Subscribe for Updates" form at the bottom of the page.
This will initially subscribe you to all mailings from IGEL, but using the unsubscribe link at the bottom of a mail, you can select which communications you wish to receive and which not.

IGEL Security Notices (ISN)

1 http://igel.com

ISN 2022-21: Chromium Vulnerability

First published 15 September 2022

CVSS 3.1 High

CVSS:3.1 n/a

Summary

A vulnerability has been found in the Chromium web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 11

Details

A vulnerability has been found in the Mojo library collection used in Chromium (CVE-2022-3075). It is rated high and is caused by insufficient data validation. Google is aware of reports that an exploit for this issue exists in the wild.

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.08.200 (release planned for mid-October)

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/09/stable-channel-update-for-desktop.html

ISN 2022-20: Firefox ESR Vulnerabilities

First published 15 September 2022

CVSS 3.1 High

CVSS:3.1 n/a

Summary

Multiple vulnerabilities have been found in the Firefox ESR web browser used in IGEL OS. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

Three vulnerabilities rated high have been found in Firefox ESR. An attacker could abuse XSLT error handling to associate attacker-controlled content with another origin which was displayed in the address bar. This could have been used to fool the user into submitting data intended for the spoofed origin (CVE-2022-38472). Another vulnerability affects a cross-origin iframe referencing an XSLT document – it would inherit the parent domain's permissions such as microphone or camera access (CVE-2022-38473). The third issue concerns memory safety bugs that could be exploited to run arbitrary code (CVE-2022-38478).

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.08.200 (release planned for mid-October)
- IGEL OS 10: Upgrade to the fixed IGEL OS 11 version

References

- Mozilla Foundation Security Advisory 2022-35: https://www.mozilla.org/en-US/security/advisories/mfsa2022-35/

ISN 2022-19: Log4j 1.x Remainder in UMS

Updated 17 October 2022 (UMS version 6.10.130 available)

First published 12 September 2022

CVSS 3.1: 3.4 (Low)

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:L

Summary

Universal Management Suite (UMS) has been found to still contain an obsolete and vulnerable Log4j version.
Affected products:

- UMS on Windows with High Availability (HA) option installed
- UMS on Linux, default installation

Details

Although IGEL has replaced most of Log4j in UMS with a different logging solution, UMS up to version 6.10.120 still contains an instance of Log4j version 1.x. It is located at `messageservice/lib/optional/log4j-1.2.14.jar` in the UMS installation directory.

This version is unmaintained, and the application's confidentiality and availability could have a low impact due to the vulnerabilities associated with version 1.x.

ⓘ UMS contains further files with log4j in their filenames, such as `log4j-api-2.17.1.jar`. These are no indicator of vulnerable Log4j versions being present. Rather, they are API bridges used by IGEL to replace Log4j with a different logging solution. They pose no risk.

Do not delete files from IGEL UMS installations. This will break the application.

Update Instructions

- Update to UMS version 6.10.130

References

- Apache Software Foundation Blog, "Apache™ Logging Services™ Project announces Log4j™ 1 end-of-life; recommends upgrade to Log4j 2": https://news.apache.org/foundation/entry/apache_logging_services_project_announces

ISN 2022-18: Linux Kernel Vulnerability

First published 7 September 2022

CVSS 3.1 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A vulnerability has been found in the Linux kernel used by IGEL OS. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

A use-after-free vulnerability has been discovered in the Netfilter subsystem in the Linux kernel (CVE-2022-32250, formerly also known as CVE-2022-1966). It is rated high and allows a local non-privileged user to escalate their privileges to root.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.08.100 or newer.
- IGEL OS 10: Upgrade to the fixed IGEL OS 11 version.

References

- CVE-2022-32250: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-32250

ISN 2022-17: Chromium WebRTC Vulnerability

Updated 30 August 2022 (IGEL OS 11.08.100 available)

First published 22 July 2022

CVSS 3.1 High

CVSS: n/a

Summary

Multiple vulnerabilities have been found in the Chromium web browser. This affects the following IGEL products:

- IGEL OS 11

Details

Google has reported a heap buffer overflow in the WebRTC component (CVE-2022-2294), which is used for multimedia and video conferencing. Google has rated this as high and states that an exploit for this issue exists in the wild. The other vulnerability rated high is a type confusion in the V8 JavaScript engine (CVE-2022-2295).

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.08.100 or newer.

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/07/stable-channel-update-for-desktop.html

ISN 2022-16: Firefox Vulnerabilities

Updated 1st July 2022 (IGEL OS 11.07.170 available)

First published 24th June 2022

CVSS 3.1 Critical

CVSS:3.1 n/a

Summary

Critical vulnerabilities have been found in the Firefox ESR browser. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

It has been discovered that an attacker who could corrupt the methods of an Array object in JavaScript via prototype pollution could execute attacker-controlled JavaScript code in a privileged context (CVE-2022-1802). In addition, an attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process (CVE-2022-1529). Both issues are considered critical.
Update instructions

- IGEL OS 11: Update to IGEL OS 11.07.170, which contains Firefox ESR 91.9.1.
- IGEL OS 10: Upgrade to IGEL OS 11.07.170.

References

Mozilla Foundation Security Advisory 2022-19: https://www.mozilla.org/en-US/security/advisories/mfsa2022-19/

ISN 2022-15: Chromium Browser Vulnerabilities

Updated 1st July 2022 (IGEL OS 11.07.170 available)

First published 20th June 2022

CVSS 3.1 Critical

CVSS:3.1 n/a

Summary

The Chromium project has reported multiple vulnerabilities in its web browser. These affect the following IGEL products:

- IGEL OS 11

Details

It has been discovered that the Indexed DB component in Chromium contains a use-after-free error. The project rates this vulnerability as critical (CVE-2022-1853). Eight further memory management issues, mostly use-after-free, exist in several other Chromium components. These have been rated as high (CVE-2022-1854, CVE-2022-1855, CVE-2022-1856, CVE-2022-1857, CVE-2022-1858, CVE-2022-1859, CVE-2022-1860, CVE-2022-1861).

Besides that, several vulnerabilities rated as medium and low exist in Chromium. They are listed in the referenced update from the Chrome Team.

Update instructions

- IGEL OS 11: Update to IGEL OS 11.07.170, which contains Chrome 102.

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_24.html
- CVE-2022-1853: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1853

ISN 2022-14: Chromium Browser Vulnerabilities

First published 3rd June 2022

CVSS 3.1 High

CVSS:3.1 n/a

Summary

The Chromium project has reported multiple vulnerabilities in its web browser. These affect the following IGEL products:

- IGEL OS 11

Details

An inappropriate implementation in Web Contents has been found in Chromium and has been rated as high (CVE-2022-1637). In addition, there are 6 issues of use-after-free which are rated high (CVE-2022-1633, CVE-2022-1634, CVE-2022-1635, CVE-2022-1636, CVE-2022-1639, CVE-2022-1640) and one such issue rated medium (CVE-2022-1641). Besides that, a heap buffer overflow has been found in V8 internationalization and rated high (CVE-2022-1638).

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.07.140, which contains Chromium version 101 or newer.

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/05/stable-channel-update-for-desktop_10.html
- CVE-2022-1637: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1637
- CVE-2022-1638: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1638

ISN 2022-13: UMS Vulnerabilities

Updated 8th June (clarification of update availability)

First published 25th May 2022

CVSS 3.1 Base Score: 8.6 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Summary

Several security issues have been found in IGEL Universal Management Suite (UMS). This affects the following IGEL products:

- UMS 6.x

Details

It has been discovered that IGEL UMS on Windows stores superuser/database credentials in the `HKEY_LOCAL_MACHINE` registry, which allows a low-privileged attacker with Operating System (OS) access to read the encrypted `dbpassword` value (CVE-2022-25804).

Another vulnerability is a hardcoded DES key which allows an attacker with access to an encrypted `dbpassword` value to decrypt the password and gain superuser/database access to IGEL UMS and its database (CVE-2022-25806).

Another hardcoded DES key allows an attacker with access to encrypted LDAP bind credentials to decrypt the password and obtain access to plaintext LDAP bind credentials (CVE-2022-25807).

Finally, UMS may expose Lightweight Directory Access Protocol (LDAP) bind credentials in plaintext form, which allows a remote, authenticated attacker to obtain access to those credentials (CVE-2022-25805).

These issues were found by Nick Nam of Atredis Partners.

Mitigations

- CVE-2022-25804 can be mitigated by using a dedicated host for the UMS server and restricting access to it to the UMS administrator only. Using a dedicated host per service is a general IT Best Practice.
- CVE-2022-25806 and CVE-2022-25807 can be mitigated by restricting access to the UMS database and its backups.
- CVE-2022-25805 can be mitigated by using LDAPS (with TLS) only, which is configurable in UMS.

Update Instructions

- UMS 6.x: A UMS release with fixes is in preparation. When it is available, this ISN will be updated.

References

- Atredis Partners, Multiple Vulnerabilities in IGEL Universal Management Suite (UMS) v6.07.100: https://github.com/atredispartners/advisories/blob/master/ATREDIS-2022-0002.md
- CVE-2022-25804: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25804
- CVE-2022-25806: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25806
- CVE-2022-25807: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25807
- CVE-2022-25805: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25805

ISN 2022-12: Teradici PCoIP Library Vulnerabilities

Updated 2nd June 2022 (IGEL OS 11.07.140 available)

First published 9th May 2022

CVSS 3.1 Base Score: High

CVSS:3.1 n/a

Summary

Multiple vulnerabilities have been found in libraries bundled with the Teradici PCoIP client for Linux. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

The Libexpat version bundled with the Teradici PCoIP client for Linux is affected by three critical issues (CVE-2022-22822, CVE-2022-22823, and CVE-2022-22824) and five issues rated high. Overall, the vendor HP rates the severity in the product context as high.

The OpenSSL version bundled with the Teradici PCoIP client for Linux has one issue rated high (CVE-2022-0778) and one rated medium (CVE-2021-4160). Overall, the vendor HP rates the severity in the product context as high.

The full list of CVEs can be found in the HP advisories given in the References section.

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.07.140 or newer.
- IGEL OS 10: Upgrade to IGEL OS version 11.07.140 or newer.

References

- HP, „Expat Library update for Teradici PCoIP Software and Firmware“: https://support.hp.com/us-en/document/ish_6052753-6052783-16/hpsbhf03750
- HP, “OpenSSL update for Teradici PCoIP”: https://support.hp.com/us-en/document/ish_6052720-6052798-16/hpsbhf03784

ISN 2022-11: VMware Horizon Privilege Escalation

Updated 2nd June 2022 (IGEL OS 11.07.140 available)

First published 26th April 2022

CVSS 3.1 Base Score: 7.3 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Summary

Two vulnerabilities have been found in VMware Horizon Client for Linux. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

The first issue (CVE-2022-22962) allows a local non-privileged user to change the default shared folder location due to a vulnerable symbolic link. This can result in linking to a file owned by root.
The second issue (CVE-2022-22964) lets a local non-privileged user escalate their privileges to root due to a vulnerable configuration file.

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.07.140 or newer.
- IGEL OS 10: Upgrade to IGEL OS version 11.07.140 or newer.

Mitigation

This issue can be mitigated by not giving users access to a terminal/virtual console on IGEL OS, which they could use to configure and run the exploit code:

Remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Or password-protect the local terminal with the Administrator password:

1. Find the local terminal session under **Accessories > Terminals**.
2. Follow the instructions under Password-Protecting Sessions and Accessories.

Disable virtual console access:

1. In IGEL Setup, go to **User Interface > Display > Access Control**.
2. Activate **Disable console switching** (Default: Console switching enabled)
3. Click **Apply**.

References

VMSA-2022-0012: https://www.vmware.com/security/advisories/VMSA-2022-0012.html

ISN 2022-10: Firefox Vulnerabilities

Updated 2nd June 2022 (IGEL OS 11.07.140 available)

First published 19th April 2022

CVSS 3.1 Base Score: 7.5 (High)

CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Multiple vulnerabilities have been found in the Firefox ESR Browser. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

The Firefox ESR Browser used in IGEL OS is affected by seven security issues rated as high. This includes a browser window spoof using fullscreen mode (CVE-2022-26383) and a bypass for the JavaScript sandbox in iframes (CVE-2022-26384). Another vulnerability affects the verification of add-on signatures: When installing an add-on, Firefox verifies the signature before prompting the user; but while the user is confirming the prompt, the underlying add-on file can be modified, and Firefox would not notice (CVE-2022-26387). The other defects concern memory safety. A full list of CVEs is available in the Mozilla advisories listed in "References".

Mitigation

CVE-2022-26387 can be mitigated by not installing new add-ons until a fixed version of Firefox ESR has been installed.

Update Instructions

- IGEL OS 11: Update to IGEL OS version 11.07.140 or newer.
- IGEL OS 10: Upgrade to IGEL OS version 11.07.140 or newer.

References

- Mozilla Foundation Security Advisory 2022-14: https://www.mozilla.org/en-US/security/advisories/mfsa2022-14/
- Mozilla Foundation Security Advisory 2022-11: https://www.mozilla.org/en-US/security/advisories/mfsa2022-11/

ISN 2022-09: Zlib Vulnerability

Updated 29th April 2022 (IGEL OS 11.07.110 available)

First published 8th April 2022

CVSS 3.1 Base Score: 8.2 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H

Summary

A vulnerability has been found in the Zlib compression library. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

When compressing specially crafted input, Zlib can run into an error that causes memory corruption, could crash applications, and could potentially lead to code execution. This issue has been registered as CVE-2018-25032 and is rated as high.

Update instructions

- IGEL OS 11: Update to IGEL OS 11.07.110 or newer.
- IGEL OS 10: Upgrade to IGEL OS 11.07.110 or newer.

References

CVE-2018-25032: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-25032

ISN 2022-08: Chromium JavaScript Vulnerability

Updated 29th April 2022 (IGEL OS 11.07.110 available)

First published 28th March 2022

Base Score: High

CVSS:3.1 vector not available yet

Summary

A vulnerability has been found in the Chromium browser. This affects the following IGEL products:

- IGEL OS 11

Details

It has been discovered that Chromium's JavaScript engine contains a vulnerability (CVE-2022-1096) that can be exploited when the user visits a web page that is under the control of an attacker. Google rates this issue as high and reports that it is being actively exploited in the wild.

Mitigation

- Use the Firefox Browser in IGEL OS 11.07.100 as an alternative, which is secured by AppArmor.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.07.110 or newer.

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_25.html
- CVE-2022-1096: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1096

ISN 2022-07: Chromium Browser Vulnerabilities

First published 22nd March 2022

CVSS 3.1 Base Score: 9.8 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

The Chromium project has reported multiple vulnerabilities in its web browser. These affect the following IGEL products:

- IGEL OS 11

Details

It has been discovered that the renderer in Chromium contains a use-after-free vulnerability which is rated critical (CVE-2022-0971). Eight further memory corruption issues have been reported which are rated high (CVE-2022-0972, CVE-2022-0973, CVE-2022-0974, CVE-2022-0975, CVE-2022-0976, CVE-2022-0977, CVE-2022-0978, CVE-2022-0979), and one medium (CVE-2022-0980).

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.07.100 (to be released on March 29th)

References

- Chrome Team – Stable Channel Update for Desktop: https://chromereleases.googleblog.com/2022/03/stable-channel-update-for-desktop_15.html
- CVE-2022-0971: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0971

ISN 2022-06: OpenSSL Denial of Service

First published 21st March 2022

CVSS 3.1 Base Score: 7.5 (High)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Summary

A vulnerability has been found in the OpenSSL cryptography library. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

It has been discovered that OpenSSL can run into an infinite loop when parsing a TLS certificate or key that has invalid explicit elliptic curve parameters (CVE-2022-0778). An attacker could use a crafted and self-signed certificate to cause a denial of service in OpenSSL and consequently in applications that use OpenSSL.

Mitigation

The attack relies on a TLS server certificate crafted by an attacker. Until the security fix is available, only connect to servers under control of your own organization or a trusted party.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.07.100 (to be released on March 29th)
- IGEL OS 10: Upgrade to IGEL OS 11.07.100 (to be released on March 29th)

References

- OpenSSL Security Advisory - Infinite loop in BN_mod_sqrt() reachable when parsing certificates (CVE-2022-0778): https://www.openssl.org/news/secadv/20220315.txt
- CVE-2022-0778: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778

ISN 2022-05: Netfilter Escalation of Privilege

First published 14th March 2022

CVSS 3.1 Base Score: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A vulnerability has been found in the Netfilter component in the Linux kernel. This affects the following IGEL products:

- IGEL OS 11

Details

An out-of-bounds (OOB) memory access flaw has been found in the Netfilter code of the Linux kernel (CVE-2022-25636). This can enable an unprivileged local user to escalate their privileges or crash the system.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.07.100 (to be released on March 29th)

Mitigation

This issue can be mitigated by not giving users access to a terminal/virtual console on IGEL OS, which they could use to configure and run the exploit code:

Remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Or password-protect the local terminal with the Administrator password:

1. Find the local terminal session under **Accessories > Terminals**.
2. Follow the instructions under Password-Protecting Sessions and Accessories.

Disable virtual console access:

1. In IGEL Setup, go to **User Interface > Display > Access Control**.

2. Activate **Disable console switching** (Default: Console switching enabled)
3. Click **Apply**.

References

- CVE-2022-25636: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25636

ISN 2022-04: Dirty Pipe Escalation of Privilege

First published 10th March 2022

CVSS 3.1 Base Score: 8.4 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

A vulnerability in the Linux kernel, nicknamed "Dirty Pipe", affects the following IGEL products:

- IGEL OS 11

Details

Dirty Pipe (CVE-2022-0847) is a vulnerability that has been found in Linux kernels since version 5.8. It enables an unprivileged local user to write to files that should be writeable for root only. By adding commands to root's cron jobs or adding lines to the `/etc/passwd` file, for example, the attacker could escalate privilege and become root on the system.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.07.100.

Mitigation

This issue can be mitigated by not giving users access to a terminal/virtual console on IGEL OS, which they could use to configure and run the exploit code:

Remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Or password-protect the local terminal with the Administrator password:

1. Find the local terminal session under **Accessories > Terminals**.
2. Follow the instructions under Password-Protecting Sessions and Accessories.

Disable virtual console access:

1. In IGEL Setup, go to **User Interface > Display > Access Control**.
2. Activate **Disable console switching** (Default: Console switching enabled)
3. Click **Apply**.

References

- CVE-2022-0847: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0847
- Max Kellerman, “The Dirty Pipe Vulnerability”: https://dirtypipe.cm4all.com

ISN 2022-03: Glibc Denial of Service in IGEL OS

First published 9th March 2022

CVSS 3.1 Base Score: 8.1 (High)

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Multiple vulnerabilities have been found in the GNU C Library (glibc). This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

Security issues have been discovered in Glibc features such as iconv (CVE-2016-10228, CVE-2019-25013, CVE-2020-27618, CVE-2020-29562, CVE-2021-3326), nscd (CVE-2021-27645) and sunrpc (CVE-2022-23218, CVE-2022-23219). A remote attacker could use these to cause the GNU C Library to hang or crash, resulting in a denial of service. Additionally, the features wordexp (CVE-2021-35942) and realpath (CVE-2021-3998) could be made to disclose information. The vulnerability in getcwd (CVE-2021-3999) could possibly be used to execute arbitrary code.

Update Instructions

- IGEL OS 11: Update to version 11.07.100 (to be released on 29th March 2022) or newer
- IGEL OS 10: Upgrade to IGEL OS 11.07.100 (to be released on 29th March 2022) or newer

Mitigation

- The issues CVE-2022-23218 and CVE-2022-23219 in sunrpc can be mitigated by mounting NFS shares from trusted NFS servers only.

References

- USN-5310-1: GNU C Library vulnerabilities: https://ubuntu.com/security/notices/USN-5310-1
- CVE-2016-10228: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10228
- CVE-2019-25013: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-25013
- CVE-2020-27618: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27618
- CVE-2020-29562: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29562
- CVE-2021-3326: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3326
- CVE-2021-27645: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-27645
- CVE-2022-23218: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23218
- CVE-2022-23219: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23219
- CVE-2021-35942: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-35942

- CVE-2021-3998: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3998
- CVE-2021-3999: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-3999

ISN 2022-02: UEFI Vulnerabilities in UD Devices

Updated 21 July 2022 (IGEL OS 11.08.100 will bring remediation)

Updated 24 February 2022 (updated "Update Instructions")

First published 10 February 2022

CVSS 3.1 Base Score: 8.2 (High)

CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Summary

Multiple vulnerabilities have been found in UEFI firmware. Several of these also affect the Insyde H2O UEFI firmware used on some IGEL devices. Insyde have not completed their investigation fully, but at present the following IGEL devices are affected:

- UD3-LX 60 (M350C)
- UD7-LX 20 (H860C)

Details

The Insyde H2O UEFI firmware contains multiple memory management vulnerabilities in System Management Mode (SMM). A local attacker with administrator privileges could use these vulnerabilities to elevate their privileges above the installed operating system in order to execute code in SMM mode. This could enable the attacker to invalidate hardware security features such as UEFI Secure Boot, install persistent malware, or create backdoors for information disclosure.

Update Instructions

- IGEL OS 11.08.100 (planned to be released in mid-August) will provide a method of deploying the UEFI updates from UMS via network.

Mitigation

- Set a UEFI password, see Ein UEFI-Passwort festlegen.
- Activate UEFI Secure Boot (default on IGEL UD devices), see UEFI Secure Boot Enabling Guides(see page 73).
- Do not allow booting from USB storage media, see USB-Boot deaktivieren.

This issue can be mitigated further by not giving users access to a terminal/virtual console on IGEL OS, which they could use to configure and run exploit code:

Remove an existing local terminal session

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.

3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Or password-protect the local terminal with the Administrator password

1. Find the local terminal session under **Accessories > Terminals**.
2. Follow the instructions under Sitzungen und Zubehör mit Passwörtern schützen.

Disable virtual console access

1. In IGEL Setup, go to **User Interface > Display > Access Control**.
2. Activate **Disable console switching**. (Default: Console switching enabled)
3. Click **Apply**.

References

- Insyde Software Security Advisory, listing all related CVEs: https://www.insyde.com/security-pledge
- CERT Coordination Center, “InsydeH2O UEFI software impacted by multiple vulnerabilities in SMM”: https://kb.cert.org/vuls/id/796611

ISN 2022-01: Polkit Escalation of Privilege

Updated 7 February 2022 (IGEL OS 11.06.250 released)

First published 27 January 2022

CVSS 3.1 Base Score: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Summary

A vulnerability has been found in Polkit, a software component that allows users to execute programs as another user - often as root, - after providing a password. This affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

Polkit (formerly known as PolicyKit) has a privilege escalation vulnerability that allows an attacker with regular user privileges to become root without a password. This vulnerability (CVE-2021-4034), nicknamed PwnKit, has been rated as high. A working proof-of-concept exploit is available on the Internet.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.06.250.
- IGEL OS 10: Upgrade to IGEL OS 11.06.250.

Mitigation

This issue can be mitigated by not giving users access to a terminal/virtual console on IGEL OS, which they could use to configure and run the exploit code:

Remove an existing local terminal session:

1. In IGEL Setup, go to **Accessories > Terminals**.
2. Select a local terminal session you want to delete.
3. Click the trash icon to remove the selected session.
4. When prompted, confirm that you want to delete the session.
5. Click **Apply**.

Or password-protect the local terminal with the Administrator password:

1. Find the local terminal session under **Accessories > Terminals**.
2. Follow the instructions under Password-Protecting Sessions and Accessories.

Disable virtual console access:

1. In IGEL Setup, go to **User Interface > Display > Access Control**.
2. Activate **Disable console switching** (Default: Console switching enabled)
3. Click **Apply**.

References

- CVE-2021-4034: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4034
- Qualys Security Advisory: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt

ISN 2021-11: UMS Log4j Vulnerability

Updated 14 February 2022 (corrected statements on CVE-2021-4104)

Updated 12 January 2022 (added CVE-2921-44832 and note on ICG)

Updated 22 December 2021 (updated CVEs, removed mitigations, added fixed UMS version)

Updated 16 December 2021 (added affected versions, corrected mitigation for Elasticsearch on Windows)

First published 13 December 2021

CVSS 3.1 Base Score:10.0 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

A critical vulnerability, also known as Log4shell, has been found in the Log4j logging library. This affects the following IGEL products (other IGEL products are not affected):

- IGEL Universal Management Suite (UMS), all versions since 5.09.100

Details

The versions 2.0-beta9 up to 2.14.1 of the Log4j library are vulnerable to Remote Command Execution (CVE-2021-44228). This means that a remote attacker can execute commands over the network on software that contains the vulnerable Log4j versions. IGEL UMS and the Elasticsearch engine in the IGEL UMS Web App are affected.

Exploit code is already available, and the issue is being actively exploited on the Internet. Therefore, IGEL strongly recommends updating all UMS installations.

In a typical UMS installation, this issue is mitigated by the fact that UMS is not reachable from the Internet.

In early attempts to fix CVE-2021-44228, further vulnerabilities have been found and assigned the identifiers CVE-2021-45046 and CVE-2021-45105. These affect the Context Lookup feature in Log4j, which UMS does not use, therefore UMS is not affected by these. Also, UMS is not affected by CVE-2021-44832, as it does not use the vulnerable features in Log4j version 2.17.

In addition, a vulnerability has been found in Log4j version 1.2.17 (CVE-2021-4104), which does not affect UMS, as the CVE applies only “when the attacker has write access to the Log4j configuration”, which is not the case in UMS.

> **Note on ICG**
> IGEL Cloud Gateway 2.04.100 contains Log4j version 1.2.17, but it is not affected by CVE-2021-4104, as it applies only “when the attacker has write access to the Log4j configuration”, which is not the case in ICG.

Update Instructions

- Update to UMS 6.09.120, which contains Log4j version 2.17

Mitigation

Older mitigation measures have been discredited. The safest course of action is to update to the fixed version.

References

- Log4j - Apache Log4j Security Vulnerabilities: https://logging.apache.org/log4j/2.x/security.html
- CVE-2021-44228: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44228
- CVE-2021-45046: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45046
- CVE-2021-45045: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-45045
- CVE-2021-4104: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-4104
- CVE-2021-44832: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-44832

ISN 2021-10: Chromium vulnerabilities

First published 30 November 2021

CVSS 3.1 Base Score: 9.8 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Summary

Many vulnerabilities have been found in the Chromium web browser, some rated as critical. These affect the following IGEL products:

- IGEL OS 11

Details

The Chromium project has reported many vulnerabilities in its browser, including issues graded as critical and high.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.06.210.

References

CVE-2021-37973, CVE-2021-37972, CVE-2021-37971, CVE-2021-37970, CVE-2021-37969, CVE-2021-37968, CVE-2021-37967, CVE-2021-37966, CVE-2021-37965, CVE-2021-37964, CVE-2021-37963, CVE-2021-37962, CVE-2021-37961, CVE-2021-37960, CVE-2021-37959, CVE-2021-37958, CVE-2021-37957, CVE-2021-37956, CVE-2021-30633, CVE-2021-30632, CVE-2021-30631, CVE-2021-30630, CVE-2021-30629, CVE-2021-30628, CVE-2021-30627, CVE-2021-30626, CVE-2021-30625, CVE-2021-30624, CVE-2021-30623, CVE-2021-30622, CVE-2021-30621, CVE-2021-30620, CVE-2021-30619, CVE-2021-30618, CVE-2021-30617, CVE-2021-30616, CVE-2021-30615, CVE-2021-30614, CVE-2021-30613, CVE-2021-30612, CVE-2021-30611, CVE-2021-30610, CVE-2021-30609, CVE-2021-30608, CVE-2021-30607, CVE-2021-30606, CVE-2021-30604, CVE-2021-30603, CVE-2021-30602, CVE-2021-30601, CVE-2021-30600, CVE-2021-30599, CVE-2021-30598, CVE-2021-30597, CVE-2021-30596, CVE-2021-30594, CVE-2021-30593, CVE-2021-30592, CVE-2021-30591, CVE-2021-30590, CVE-2021-30589, CVE-2021-30588, CVE-2021-30587, CVE-2021-30586, CVE-2021-30585, CVE-2021-30584, CVE-2021-30583, CVE-2021-30582, CVE-2021-30581, CVE-2021-30580, CVE-2021-30579, CVE-2021-30578, CVE-2021-30577, CVE-2021-30576, CVE-2021-30575, CVE-2021-30574, CVE-2021-30573, CVE-2021-30572, CVE-2021-30571, CVE-2021-30569, CVE-2021-30568, CVE-2021-30567, CVE-2021-30566, CVE-2021-30565, CVE-2021-37976, CVE-2021-37975, CVE-2021-37974, CVE-2021-37977, CVE-2021-37979, CVE-2021-37980, CVE-2021-37981, CVE-2021-37982, CVE-2021-37983, CVE-2021-37984, CVE-2021-37985, CVE-2021-37986, CVE-2021-37987, CVE-2021-37988, CVE-2021-37989, CVE-2021-37990, CVE-2021-37991, CVE-2021-37992, CVE-2021-37993, CVE-2021-37996, CVE-2021-37994, CVE-2021-37995, CVE-2021-38003, CVE-2021-38002, CVE-2021-38001, CVE-2021-38000, CVE-2021-37999, CVE-2021-37998 and CVE-2021-37997.

ISN 2021-09: Firefox ESR vulnerabilities

First published 30 November 2021

CVSS 3.1 Base Score: 10.0 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

Several vulnerabilities have been found in Mozilla Firefox ESR, many rated as high. These affect the Firefox ESR version in the following IGEL products:

IGEL OS 11

IGEL OS 10

Details

Mozilla has reported various vulnerabilities in Firefox ESR in its Mozilla Foundation Security Advisories (MFSA-2021-49, MFSA-2021-45, MFSA-2021-40, MFSA-2021-37, MFSA-2021-33). Many concern memory safety, and many are exploitable over the network. Overall, 18 are rated high.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.06.210.
- IGEL OS 10: Upgrade to IGEL OS 11.06.210.

References

- MFSA-2021-49: https://www.mozilla.org/en-US/security/advisories/mfsa2021-49/
  CVE-2021-38503, CVE-2021-38504, CVE-2021-38506, CVE-2021-38507, MOZ-2021-0008, CVE-2021-38508, CVE-2021-38509, MOZ-2021-0007. (MOZ-* pending CVE assignment)
- MFSA-2021-45: https://www.mozilla.org/en-US/security/advisories/mfsa2021-45/
  CVE-2021-38496, CVE-2021-38497, CVE-2021-38498, CVE-2021-32810, CVE-2021-38500, CVE-2021-38501
- MFSA-2021-40: https://www.mozilla.org/en-US/security/advisories/mfsa2021-40/
  CVE-2021-38495
- MFSA-2021-37: https://www.mozilla.org/en-US/security/advisories/mfsa2021-37/
  CVE-2021-29991
- MFSA-2021-33: https://www.mozilla.org/en-US/security/advisories/mfsa2021-33/
  CVE-2021-29986, CVE-2021-29981, CVE-2021-29988, CVE-2021-29984, CVE-2021-29980, CVE-2021-29987, CVE-2021-29985, CVE-2021-29982, CVE-2021-29989, CVE-2021-29990

ISN 2021-08: ICG Authentication Vulnerability

First published 17 November 2021

CVSS 3.1 Base Score: 10.0 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Summary

A critical security vulnerability affects IGEL Cloud Gateway (ICG) in the following versions:

- All ICG versions before 2.04.100

Details

A penetration test has found an authentication vulnerability in ICG. It could enable an unauthenticated remote attacker to send commands and settings to connected IGEL OS endpoints.

IGEL would like to thank SCHUTZWERK GmbH, who discovered the vulnerability.

Update Instructions

- Update to ICG 2.04.100.

ISN 2021-07: UMS Web App Information Disclosure

First published 27 September 2021

CVSS 3.1 Base Score: 9.9 (Critical)

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:L

Summary

A critical security vulnerability in UMS Web App affects the following IGEL products:

- UMS 6.8.x with UMS Web App installed
- UMS 6.7.x with UMS Web App installed
- UMS 6.6.x with UMS Web App installed
- UMS 6.5.x with UMS Web App installed

Details

A penetration test has found that the UMS Web App can be made to reveal critical information, including the UMS Superuser password. IGEL would like to thank Lennert Preuth from SCHUTZWERK GmbH, who discovered the vulnerability.

Update Instructions

- Update to UMS 6.08.120

Mitigation

- IGEL strongly recommends that all affected users update/upgrade to UMS 6.08.120. If you have reasons not to do that, you can do the following:
    a. Make a UMS data backup.
    b. Re-run your current installer and re-install UMS without UMS Web App.

ISN 2021-06: IGEL OS OpenSSH Vulnerabilities

Updated 29 October 2021 (alternative mitigation for CVE-2020-15778)

Updated 23 September 2021 (IGEL OS 11.06.100 is now available)

First published 2 August 2021

CVSS 3.1 Base Score: 7.8 (High)

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Summary

Three security vulnerabilities in OpenSSH affect the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

The `scp` command in OpenSSH through 8.3p1 allows command injection in the `scp.c toremote` function, as demonstrated by backtick characters in the destination argument (CVE-2020-15778). This allows `scp` users to execute commands on the remote system. Note: The vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows." This vulnerability is rated with a CVSS 3.1 Base Score 7.8 (High).

The ssh-agent in OpenSSH before 8.5 has a double free (CVE-2021-28041) that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system (does not apply to IGEL OS), or the forwarding of an agent to an attacker-controlled host. This vulnerability is rated with a CVSS 3.1 Base Score 7.1 (High). Also, the client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation (CVE-2020-14145). This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). Note: Some reports state that 8.5 and 8.6 are also affected. This vulnerability is rated with a CVSS 3.1 Base Score 4.3 (Medium).

Update Instructions

CVE-2021-28041 is fixed in IGEL OS 11.06.100.

There are no updates yet for the other two issues.

Mitigation

- The first option for CVE-2020-15778: Unless you explicitly need the OpenSSH server on IGEL OS, disable it. It is not needed for the management of IGEL OS endpoints via UMS or ICG.
    a. In IGEL Setup, go to **System > Remote Access > SSH Access**.
    b. Uncheck the **Enable** checkbox.
    c. Click **Apply**.
    d. Reboot the system.

- The second option for CVE-2020-15778: If you use the ssh server on IGEL OS for executing commands remotely, limit command execution via the `ssh` and `scp` commands:
    a. In IGEL Setup, go to **System > Remote Access > SSH Access**.
    b. Under **User access**, make sure that **user** is set to **Deny**.
    c. Make sure that **ruser** is not denied access, and use **ruser** for ssh access.
    d. Under **Applications access for remote user 'ruser'**, add a commandline with the full Linux path of the command you want to execute. Do this for every command you want to execute via ssh.
    e. Click **Apply**.
    f. Reboot the system.
- For CVE-2020-14145: If you offer an SSH client session to your IGEL OS users, instruct them to check the remote host key fingerprint on the first connect. Supply them with the correct fingerprint for comparison.

References

- CVE-2020-15778: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-15778
- CVE-2021-28041: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28041
- CVE-2020-14145: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-14145

ISN 2021-05: IGEL OS Denial of Service

Announced 23 July 2021

Updated 23 September 2021 (IGEL OS 11.06.100 is now available)

CVSS 3.1 Score: 8.8 (High)

CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Summary

A local denial of service vulnerability affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

A research team from Qualys has discovered a vulnerability in `systemd` (CVE-2021-33910). An unprivileged local user can exploit it to crash `systemd` and the whole operating system (kernel panic).

Update Instructions

- IGEL OS 11: Upgrade to IGEL OS 11.06.100
- IGEL OS 10: Upgrade to IGEL OS 11

Mitigation

- Disable terminal access for the user, see Disabling Local Terminal Access.
- Disable virtual console access, see Disabling Virtual Console Access.
- As the attack relies on mounting user-controlled filesystems, disable mounting of filesystems by the user:
    - Disable storage hotplug (disabled by default), see Disabling Storage Hotplug.
    - Remove the Mobile Device Access USB feature (removed by default), see Removing Unused Features.

References

- Qualys, “CVE-2021-33910: Denial of Service (Stack Exhaustion) in systemd (PID 1))”: https://blog.qualys.com/vulnerabilities-threat-research/2021/07/20/cve-2021-33910-denial-of-service-stack-exhaustion-in-systemd-pid-1
- CVE-2021-33910: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33910

ISN 2021-04: IGEL OS Kernel Privilege Escalation

Announced 23 July 2021

Updated 23 September 2021 (IGEL OS 11.06.100 is now available)

CVSS 3.1 Score: 7.8 (High)

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Summary

A local privilege escalation vulnerability affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

A research team from Qualys has discovered a vulnerability in the Linux kernel's filesystem layer (CVE-2021-33909). An unprivileged local user can use it to gain root privileges.

Update Instructions

- IGEL OS 11: Upgrade to IGEL OS 11.06.100
- IGEL OS 10: Upgrade to IGEL OS 11

Mitigation

- Disable terminal access for the user, see Disabling Local Terminal Access.
- Disable virtual console access, see Disabling Virtual Console Access.
- As the attack relies on mounting user-controlled filesystems, disable mounting of filesystems by the user:
    - Disable storage hotplug (disabled by default), see Disabling Storage Hotplug.
    - Remove the Mobile Device Access USB feature (removed by default), see Removing Unused Features.
- Qualys has published mitigations for the specific exploit that their researchers used (other exploitation techniques may exist): https://blog.qualys.com/vulnerabilities-threat-research/2021/07/20/sequoia-a-local-privilege-escalation-vulnerability-in-linuxs-filesystem-layer-cve-2021-33909

References

- Qualys, "Sequoia: A Local Privilege Escalation Vulnerability in Linux's Filesystem Layer (CVE-2021-33909)": https://blog.qualys.com/vulnerabilities-threat-research/2021/07/20/sequoia-a-local-privilege-escalation-vulnerability-in-linuxs-filesystem-layer-cve-2021-33909

- CVE-2021-33909: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-33909

ISN 2021-03: IGEL W10 Print Spooler Vulnerability

First published 7 July 2021
Updated 15 October 2021 (private build with security fixes available from IGEL)
Updated 16 July 2021 (inserted update instructions)

CVSS 3.1 Score: 8.8 (High)
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

A Remote Code Execution (RCE) vulnerability, known as PrintNightmare, affects the following IGEL products:

- IGEL W10 IoT

Details

A remote code execution vulnerability (CVE-2021-34527) exists when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges.

Update Instructions

1. IGEL customers can request the private build (PB) W10 IoT 4.04.180 from IGEL Customer Engineering (https://support.igel.com/csm), which contains the needed security fixes.
2. Install the update.
3. In addition to installing the update, in order to secure your system, you must confirm that the following registry settings are set to 0 (zero) or are not defined. In the default IGEL setting, they do not exist and therefore are in the secure setting already. You can check and set them by opening the Command Prompt and issuing the “regedit” command.
    - `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint`
    - `NoWarningNoElevationOnInstall = 0 (DWORD)` or `not defined` (default setting)
    - `UpdatePromptSettings = 0 (DWORD)` or `not defined` (default setting)
      Microsoft warns that having `NoWarningNoElevationOnInstall` set to “1” makes your system vulnerable by design.

References

- CVE-2021-34527: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34527
- Microsoft, “Windows Print Spooler Remote Code Execution Vulnerability”: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527
- Microsoft, “Windows Print Spooler Remote Code Execution Vulnerability”: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958

ISN 2021-02: IGEL OS and W10 Wi-Fi Vulnerabilities (Fragattacks)

First published 21 May 2021

Updated 30 September 2021 (Resolution in IGEL OS 11.06.100)

CVSS 3.1 Score: 5.0 (Medium)
CVSS:3.1/AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

Several Wi-Fi vulnerabilities, known collectively as Fragattacks, affect the following IGEL products:

- IGEL OS 11
- IGEL OS 10
- IGEL W10 IoT

Details

The researcher Mathy Vanhoef has found several security vulnerabilities both in the IEEE 802.11 standards underpinning Wi-Fi and their implementations in Linux and Windows. He has demonstrated that weaknesses in the fragmentation and frame aggregation mechanisms can be abused to exfiltrate confidential data from or inject frames into a protected Wi-Fi connection between a client and the access point.

In IGEL software, these threats are mitigated as it uses TLS for endpoint management via UMS and ICG. Also, IGEL OS updates are cryptographically signed and validated. This is reflected in IGEL's CVSS 3.1 scoring of these issues.

Several CVE identifiers have been assigned to this group of vulnerabilities:

Design flaws:

- CVE-2020-24588[2]: Aggregation attack (accepting non-SPP A-MSDU frames)
- CVE-2020-24587[3]: Mixed key attack (reassembling fragments encrypted under different keys)
- CVE-2020-24586[4]: Fragment cache attack (not clearing fragments from memory when (re)connecting to a network)

Implementation vulnerabilities that allow the trivial injection of plaintext frames in a protected Wi-Fi network are assigned the following CVEs:

- CVE-2020-26140[5]: Accepting plaintext data frames in a protected network
- CVE-2020-26143[6]: Accepting fragmented plaintext data frames in a protected network

Other implementation flaws are assigned the following CVEs:

- CVE-2020-26147[7]: Reassembling mixed encrypted/plaintext fragments
- CVE-2020-26141[8]: Not verifying the TKIP MIC of fragmented frames.

2 https://nvd.nist.gov/vuln/detail/CVE-2020-24588
3 https://nvd.nist.gov/vuln/detail/CVE-2020-24587
4 https://nvd.nist.gov/vuln/detail/CVE-2020-24586
5 https://nvd.nist.gov/vuln/detail/CVE-2020-26140
6 https://nvd.nist.gov/vuln/detail/CVE-2020-26143
7 https://nvd.nist.gov/vuln/detail/CVE-2020-26147
8 https://nvd.nist.gov/vuln/detail/CVE-2020-26141

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.06.100 or newer. This fixes all design flaws and Linux implementation flaws listed above.
- IGEL OS 10: Upgrade to IGEL OS 11.06.100 or newer.

Mitigations

- If possible, replace Wi-Fi connections with wired Ethernet.

The reporter of these vulnerabilities recommends the following mitigations until fixes are available:

- Use HTTPS/TLS exclusively for websites in order to add another layer of protection for confidential information such as usernames and passwords.
  Keep your Wi-Fi access points updated with the latest firmware version.
- Reduce the impact of attacks by manually configuring your DNS server so that it cannot be poisoned.
- Specific to your Wi-Fi configuration, you can mitigate attacks (but not fully prevent them) by disabling fragmentation, disabling pairwise rekeys, and disabling dynamic fragmentation in Wi-Fi 6 (802.11ax) devices.

References

- https://www.fragattacks.com
- Mathy Vanhoef, “Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation”: https://papers.mathyvanhoef.com/usenix2021.pdf

ISN 2021-01: IGEL OS Remote Command Execution Vulnerability

Announced 25 February 2021

CVSS 3.1 Score: 9.8 (Critical)

A remote command execution (RCE) vulnerability affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

An external penetration test has found that the TLS connector service used in IGEL OS for *secure shadowing* and *secure terminal* is vulnerable to command injection. This vulnerability enables remote command execution in IGEL OS.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.04.270 or newer.
- IGEL OS 11.03.* branch: Update to version 11.03.620 or newer
- IGEL OS 10: Upgrade to IGEL OS 10.06.220 or newer.

Mitigation

Disable secure shadowing, see Shadow. However, it is not advisable to use unencrypted shadowing instead.

Disable secure terminal, see Secure Terminal.

ISN 2020-10: IGEL OS Bluetooth Vulnerabilities

Announced 8 December 2020

Score: High

Three Bluetooth vulnerabilities, one rated as high, affect the following IGEL products:

- IGEL OS 11
- IGEL OS 10

Details

Weaknesses in input validation and access control have been discovered in BlueZ, the Linux Bluetooth stack, and have been nicknamed "BleedingTooth". CVE-2020-12352 and CVE-2020-24490, both rated medium, may disclose information to an unauthenticated user nearby. CVE-2020-12351 is rated high as it may allow an unauthenticated user nearby to enable escalation of privilege.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.04.240 or newer.
- IGEL OS 10: Upgrade to IGEL OS 11.

Mitigation

Disable Bluetooth, see Bluetooth Assistant.

References

Intel BlueZ Advisory: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00435.html

ISN 2020-09: Command Execution from Start Menu

Announced 7 October 2020

Score: High

A local command execution security issue affects the start menu on:

- IGEL OS 11 (11.04.xxx before 11.04.130)

Details

A component update has added a feature to the start menu that lets unprivileged users run any command that the “User” account is allowed to execute. This enables users to break out of the limited user interface, e.g. to start a local terminal or add a session.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.04.130 or newer.

Mitigation

In IGEL Setup, go to **User Interface > Desktop > Start Menu** and set **Start menu type** to "Legacy". This removes command execution.

ISN 2020-08: Firefox ESR Various Vulnerabilities

Announced 17 September 2020

Score: High

Several security issues, 8 rated as high, affect the Firefox ESR web browser on:

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

It has been found that manipulating individual parts of a URL object could have caused an out-of-bounds read, leaking process memory to malicious JavaScript (CVE-2020-12418). Apart from that, by observing the stack trace for JavaScript errors in web workers, it was possible to leak the result of a cross-origin redirect (CVE-2020-15652. The WebRTC data channel could leak internal memory addresses to a peer, enabling them to bypass ASLR (CVE-2020-6514).
Another vulnerability allowed a malicious webpage to prompt the user to install an extension. Combined with user confusion, this could result in an unintended or malicious extension being installed (CVE-2020-15664).
Finally, a number of memory management bugs have been discovered (CVE-2020-12419, CVE-2020-12420, CVE-2020-15659, CVE-2020-15669).

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.04.130 or newer.
- IGEL OS 10: An updated version is upcoming. When it is available, this document will be updated.
- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible: https://kb.igel.com/igellinux/en/features-2275613.html

References

Mozilla Foundation Security Advisory 2020-25: https://www.mozilla.org/en-US/security/advisories/mfsa2020-25/

Mozilla Foundation Security Advisory 2020-31: https://www.mozilla.org/en-US/security/advisories/mfsa2020-31/

Mozilla Foundation Security Advisory 2020-37: https://www.mozilla.org/en-US/security/advisories/mfsa2020-37/

ISN 2020-07: Firefox ESR Various Vulnerabilities

Announced 9 June 2020

Score: High

Four security issues rated as high affect the Firefox ESR web browser on:

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

It has been discovered that a timing attack against Mozilla's Network Security Services (NSS) library could leak private keys (CVE-2020-12399). Also, when browsing a malicious page, a race condition in SharedWorkerService could occur and lead to a potentially exploitable crash (CVE-2020-12405). A JavaScript type confusion with NativeTypes could result in a crash, and potentially to execution of arbitrary code (CVE-2020-12406). Further memory safety bugs showed evidence of memory corruption and Mozilla presume that with enough effort some of these could have been exploited to run arbitrary code (CVE-2020-12411).

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.03.580 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.190 or newer.
- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible: Features.

References

Mozilla Foundation Security Advisory 2020-21: https://www.mozilla.org/en-US/security/advisories/mfsa2020-21/

ISN 2020-06: IGEL Cloud Gateway (ICG) Various Vulnerabilities

Announced 15 July 2020

Score: High

Various security issues, among them 3 rated as high, have been discovered in IGEL Cloud Gateway (ICG) before version 2.02.100.

Details

A penetration test commissioned by IGEL has found an issue in the authentication mechanism between UMS and ICG. Furthermore, there were some missing or not strict enough authorization checks in the communication between UMS, ICG and the endpoint devices. Finally, there was information disclosure in the server status response and in the ICG log files.

Update Instructions

- Update to IGEL Cloud Gateway 2.02.100 or newer.

ISN 2020-05: Intel Chipset Vulnerabilities

Announced 9 June 2020

Score: Medium

A vulnerability in Intel chipsets affects the following IGEL hardware:

- IGEL UD 2 (M250C) with BIOS versions before v3.D.13-05292019 (July 2019)
- IGEL UD 6 (H830C) with BIOS versions before v.3.3.13-05232019 (July 2019)

Details

A potential security vulnerability in Intel CPUs may allow information disclosure.

Update Instructions

IGEL OS users need not update the BIOS/UEFI. Instead, the microcode released by Intel will be applied at boot time by IGEL OS.

- IGEL OS 11: Update to IGEL OS 11.03.580 or newer
- IGEL OS 10: Update to IGEL OS 10.06.180 or newer

References

INTEL-SA-00233 “Microarchitectural Data Sampling Advisory”: https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html

ISN 2020-04: Firefox ESR Various Vulnerabilities

Announced 9 June 2020

Score: Critical

Two security issues rated critical and one rated high affect the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

A race condition when running shutdown code for Web Worker led to a use-after-free vulnerability. This resulted in a potentially exploitable crash. (CVE-2020-12387). Additionally, memory safety bugs have been reported in Firefox ESR 68.7. Some of these bugs showed evidence of memory corruption and Mozilla presume that with enough effort some of these could have been exploited to run arbitrary code (CVE-2020-12395). Furthermore, a buffer overflow could occur when parsing and validating SCTP chunks in WebRTC. This could have led to memory corruption and a potentially exploitable crash (CVE-2020-6831).

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.03.580 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.180 or newer.
- IGEL Linux v5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible: https://kb.igel.com/igellinux/en/features-2275613.html

References

Mozilla Foundation Security Advisory 2020-17: https://www.mozilla.org/en-US/security/advisories/mfsa2020-17/

ISN 2020-03: Firefox ESR Vulnerabilities

Announced 24 April 2020

Score: Critical

Two critical security issues affect the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

Under certain conditions, when running the nsDocShell destructor (CVE-2020-6819) or when handling a ReadableStream (CVE-2020-6820), race conditions can cause a use-after-free. These vulnerabilities can be exploited to inject code into Firefox memory and execute it in the web browser's context. Mozilla are aware of targeted attacks in the wild abusing these flaws.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.03.530 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.179 or newer.
- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible: https://kb.igel.com/igellinux/en/features-2275613.html

References

Mozilla Foundation Security Advisory 2020-11: https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/

ISN 2020-02: Windows CryptoAPI Spoofing Vulnerability

Announced 24 February 2020

Score: High

A high scoring security issue affects IGEL Windows 10 IoT

Details

A vulnerability has been discovered in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates (CVE-2020-0601). An attacker could exploit this to sign a malware executable with a spoofed certificate so that it will look legitimate to Windows. This vulnerability is also known as “Curve Ball” or “Chain of Fools”.

Update Instructions

- Update to IGEL Windows 10 IoT version 4.04.140 or newer.

References

NVD - CVE-2020-0601 Detail: https://nvd.nist.gov/vuln/detail/CVE-2020-0601

ISN 2020-01: Firefox ESR Vulnerability

Announced 15 January 2020

Score: Critical

A critical security issue affects the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

Incorrect alias information in IonMonkey JIT compiler for setting array elements could lead to a type confusion (memory vulnerability). Mozilla is aware of targeted attacks in the wild abusing this flaw (CVE-2019-17026).

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.03.110 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.170 or newer.
- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible: https://kb.igel.com/igellinux/en/features-2275613.html

References

Mozilla Foundation Security Advisory 2020-03: https://www.mozilla.org/en-US/security/advisories/mfsa2020-03/

ISN-2019-13: Windows Defender

Announced 17 October 2019

Score: High

A security issue affects IGEL Windows products in the following versions:

- IGEL Windows 10 IoT

Details

A denial of service vulnerability exists when Microsoft Defender improperly handles files. An attacker could exploit the vulnerability to overwrite the discretionary access control list (DACL) for a file. To exploit the vulnerability, an attacker would first require execution on the victim system.

Update Instructions

- IGEL Windows 10 IoT: Update to IGEL Windows 10 IoT 4.04.120 or newer.

References

Microsoft Security Response Center - CVE-2019-1255 | Microsoft Defender Denial of Service Vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1255

ISN-2019-12: Internet Explorer Vulnerability

Announced 08 October 2019

Score: High

A security issue affects IGEL Windows products in the following versions:

- Universal Desktop W7+
- IGEL Windows 10 IoT

Details

A remote code execution vulnerability exists in the way that the scripting engine handles objects in memory in Internet Explorer. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user.

Update Instructions

- Universal Desktop W7+: Update to version 3.14.100 or newer.
- IGEL Windows 10 IoT: Upgrade to IGEL Windows 10 IoT 4.04.120 or newer.

References

Microsoft Security Response Center - CVE-2019-1367 | Scripting Engine Memory Corruption

Vulnerability: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367

ISN 2019-11: Firefox ESR Vulnerabilities

Announced 13 September 2019

Score: High

Several security issues affect the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux v5

Details

Many vulnerabilities have been discovered in Firefox ESR, which Mozilla has summarized in the Mozilla Foundation Security Advisory (MFSA) 2019-27 with an overall critical score. The advisory contains CVE-2019-11746, CVE-2019-11744, CVE-2019-11752, CVE-2019-9812, CVE-2016-11743 and CVE-2019-11740, which include potentially exploitable crashes while manipulating video elements or extracting a key value in IndexedDB, and a sandbox escape through Firefox Sync.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.02.150 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.130 or newer.
- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends removing the web browser feature if possible: https://kb.igel.com/igellinux/en/features-2275613.html

References

Mozilla Foundation Security Advisory 2019-27: https://www.mozilla.org/en-US/security/advisories/mfsa2019-27/

ISN 2019-10: Spectre SWAPGS CPU Vulnerability

Announced 16 August 2019

Score: Low

A security issue affects Intel and AMD x86_64 CPUs.

Details

A Spectre-v1-like vulnerability using the "SWAPGS" instruction (CVE-2019-1125) has been discovered in 64-bit CPUs. It could enable a skilled local attacker to access private information via a side channel attack. This vulnerability can be mitigated by operating system updates.

IGEL assigns only a score of "Low" to this vulnerability because on IGEL operating systems there is only one non-privileged user that owns private information. A scenario of another non-privileged user using this attack to access private data is therefore not realistic.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.02.150 or newer (an earlier fix in IGEL OS 11.02.100 contains a backporting error, CVE-2019-15902).
- IGEL OS 10: Update to IGEL OS 10.06.120 or newer.
- IGEL Windows 10 IoT: Upgrade to IGEL Windows 10 IoT 4.04.110 or newer.
- Universal Desktop W7+: Update to Universal Desktop W7+ version 3.13.150 or newer.

References

Bitdefender: SWAPGS Attack: https://www.bitdefender.com/business/swapgs-attack.html

Red Hat Knowledgebase: CVE-2019-112: Spectre SWAPGS gadget vulnerability: https://access.redhat.com/articles/4329821

ISN 2019-09: IGEL OS SWP Vulnerability

Announced 24 July 2019

Score: High

A security issue affects the Shared Workplace (SWP) feature in the following IGEL OS version:

- IGEL OS 10.06.100

Details

The Shared Workplace login accepts any user credentials. However, no user settings are applied to the device.

Update Instructions

- Update to IGEL OS 10.06.110 or newer.

ISN 2019-08: Firefox ESR Vulnerabilities

Announced 24 July 2019

Score: Critical

Several security issues affect the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux v5

Details

Many vulnerabilities have been discovered in Firefox ESR, which Mozilla has summarized in the following Mozilla Foundation Security Advisories (MFSAs): MFSA-2019-22, MFSA-2019-19, MFSA- 2019-18, MFSA-2019-08, MFSA-2019-05 and MFSA-2019-02. Among these are vulnerabilities such as a sandbox escape, a script injection vulnerability, privilege escalation and some critical memory management weaknesses.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.01.130 or newer.
- IGEL OS 10: Update to IGEL OS 10.06.110 or newer.

Mitigation

- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends disabling the web browser feature if possible: https://kb.igel.com/igellinux/en/features-2275613.html

References

- MFSA-2019-22: https://www.mozilla.org/en-US/security/advisories/mfsa2019-22/
- Mozilla Foundation Security Advisories: https://www.mozilla.org/en-US/security/advisories/

ISN 2019-07: Firefox ESR Vulnerability

Announced 5 July 2019

Score: High

A security issue affects the Firefox ESR web browser on

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

Two vulnerabilities (CVE-2019-11708 and CVE-2019-11707) have been discovered in Firefox that in combination allow a remote attacker to execute code on a target machine.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.01.120, containing the fixed Firefox ESR version 60.7.2.
- IGEL OS 10: Update to IGEL OS 10.05.830, containing the fixed Firefox ESR version 60.7.2.

Mitigation

- IGEL Linux 5: This version does not have the space required for the Firefox ESR update. IGEL recommends disabling the web browser feature if possible: https://kb.igel.com/igellinux/en/features-2275613.html

ISN 2019-06: IGEL OS Kernel Vulnerability

Announced 5 July 2019

Score: High

A security issue affects IGEL Linux-based operating systems in the following versions:

- IGEL OS 11
- IGEL OS 10
- IGEL Linux 5

Details

It has been discovered that the Linux Kernel can be crashed by sending specially crafted network packets to a Linux host (CVE-2019-11477, CVE-2019-11478 and CVE-2019-11479). Issues in minimum segment size (MSS) and TCP Selective Acknowledgement (SACK) capabilities can cause a kernel panic.

Update Instructions

- IGEL OS 11: Update to IGEL OS 11.01.120
- IGEL OS 10: Update to IGEL OS 10.05.830

Mitigation

- IGEL Linux 5: Add the following command to **System > Firmware Customization > Custom Commands > Base > Initialization**: `echo 0 > /proc/sys/net/ipv4/tcp_mtu_probing ; iptables -I INPUT -p tcp -m tcpmss --mss 1:1000 -j DROP`

References

Advisory from Netflix with further suggestions for workarounds:

https://github.com/Netflix/security-bulletins/blob/master/advisories/third-party/2019-001.md

ISN 2019-05: UMS HA Vulnerability

Announced 14 June 2019

Score: High

A security issue affects Universal Management Suite (UMS) in the following versions:

- UMS 5.x if using High Availability feature
- UMS 6.x if using High Availability feature

Details

It has been discovered that a UMS component used for the High Availability (HA) feature has a debug port open. This may enable a remote attacker to read information and execute Java code in the context of the Java VM.

Update Instructions

Update to UMS 6.02.100 or newer.

To update your UMS installation, please follow these instructions: Updating UMS

ISN 2019-04: RDP Vulnerability in WES7

Announced 7 June 2019

Score: Critical

A security issue in Remote Desktop Services affects IGEL Windows Embedded Standard 7 (WES7) in all versions.

Details

Microsoft has reported a remote code execution vulnerability (CVE-2019-0708, KB4499175) in Remote Desktop Services (formerly known as Terminal Services) affecting many Windows versions up to 7. An unauthenticated attacker can remotely install programs, view, change, or delete data, or create new accounts with full user rights. This requires no user interaction and could therefore be exploited by a worm – this is why this vulnerability scores as critical.

Update Instructions

Update all your IGEL Windows Embedded Standard 7 systems to version 3.13.140.

Further Information

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

ISN 2019-03: Zombieload, RIDL, Fallout

Announced 22 May 2019

Score: Low

A security issue affects Intel-based devices running the following IGEL software products:

- IGEL OS 11
- IGEL OS 10
- IGEL Windows 10 Enterprise IoT

Details

Several vulnerabilities (CVE-2018-12126, CVE-2018-12130, CVE-2018-12127, CVE-2019-11091) affect the speculative execution features of Intel microprocessors. They can enable an attacker's code to read data from other parts of the processor, which by design should be inaccessible to it. In principle, this would allow stealing information from a different process, user or virtual machine.

However, IGEL operating systems do not run virtual machines, do not support multi-user operation and do only run preinstalled code from a read-only file system. Therefore, the impact on IGEL operating systems is low.

Update Instructions

IGEL is preparing IGEL OS 11, IGEL OS 10 and IGEL W10 firmware versions with security fixes. This ISN will be updated to inform customers when these versions become available.

IGEL W10	4.04.100 (upcoming)
IGEL OS 10	10.06.100 (upcoming)
IGEL OS 11	11.02.100 (upcoming)

ISN 2019-02: UMS Vulnerability

Overview

Announced 24 April 2019

Score: High

A security issue affects Universal Management Suite (UMS) in the following versions:

- UMS 6.x
- UMS 5.x

Details

An implementation bug in UMS user authentication allows an unauthenticated user to send commands to devices.

Update Instructions

UMS 6.x

Update to UMS 6.01.130 or newer. For instructions, see Updating UMS.

UMS 5.x

Update to UMS 5.09.140 or newer. For instructions, see Updating UMS.

ISN 2019-01: UMS Vulnerability

Overview

Announced 28 March 2019

Severity: High

A security issue affects Universal Management Suite (UMS) in the following versions:

* UMS 6.x

* UMS 5.x

Details

An implementation bug in endpoint authentication allows an endpoint to impersonate another endpoint when communicating with UMS.

IGEL would like to thank Timo Lindfors from Nixu Corporation who discovered and reported this.

Update Instructions

UMS 6.x: Update to UMS 6.01.110 or newer.

UMS 5.x: Update to UMS 5.09.130 or newer.

To update your UMS installation, please follow these instructions: Updating UMS

Product Security Archive

UMS TLS Support
Notice from 2018-05-12
Since version 5.08.100, the UMS support TLS v1.2 only.

Deprecation of Weak Algorithms
Notice from 2018-03-13
See SSH: Deprecation of Weak Algorithms as of IGEL Linux 10.04.100

IGEL Meltdown and Spectre (2)
Notice from 2018-02-01
Security fixes available for download[9]
See newsletter[10]

IGEL Meltdown and Spectre
Notice from 2018-01-18
Security fixes available for download[11]
See newsletter[12]

KRACK Attacks
Notice from 2017-10-23
Security fixes available for download[13]
See newsletter[14]

9 https://www.igel.com/software-downloads/
10 https://mailchi.mp/6ede7858d1c2/igel-technical-newsletter-january18_meltdown_spectre-1289945
11 https://www.igel.com/software-downloads/
12 http://mailchi.mp/6d07867522c2/igel-technical-newsletter-january18_meltdown_spectre-1289889
13 https://www.igel.com/software-downloads/
14 http://mailchi.mp/b68f2468dce3/igel-technical-newsletter-august-1289593

Reporting Vulnerabilities in IGEL Products

Are you a security researcher who has discovered a vulnerability in an IGEL product? Please contact security@igel.com[15] to report it. A PGP/GPG key for confidential communication is available upon request.

IGEL customers are asked, however, to open a case on the IGEL Customer Portal[16].

15 mailto:security@igel.com
16 https://support.igel.com/

UEFI Secure Boot Enabling Guides

As of IGEL OS 10.04.100, and as of Microsoft Windows 10 IoT 4.03.100, UEFI Secure Boot has been introduced to IGEL devices.

For the devices listed below, activation of UEFI Secure Boot may be needed first; for instructions, click the appropriate link:

- UD2-LX 40 (see page 75)
- UD3-LX 50 (see page 83)
- UD3-LX 51 (see page 90)
- UD6-LX 51 (see page 98)
- UD7-LX 10 (see page 106)
- UD3-W10 51 (see page 112)
- UD6-W10 51 (see page 119)
- UD7-W10 10 (see page 126)

IGEL OS

Enabling UEFI Secure Boot in UD2-LX 40

Prerequisites

- IGEL OS 10.04.100 or higher
- BIOS BayTrail.5.04.32.0022 or higher

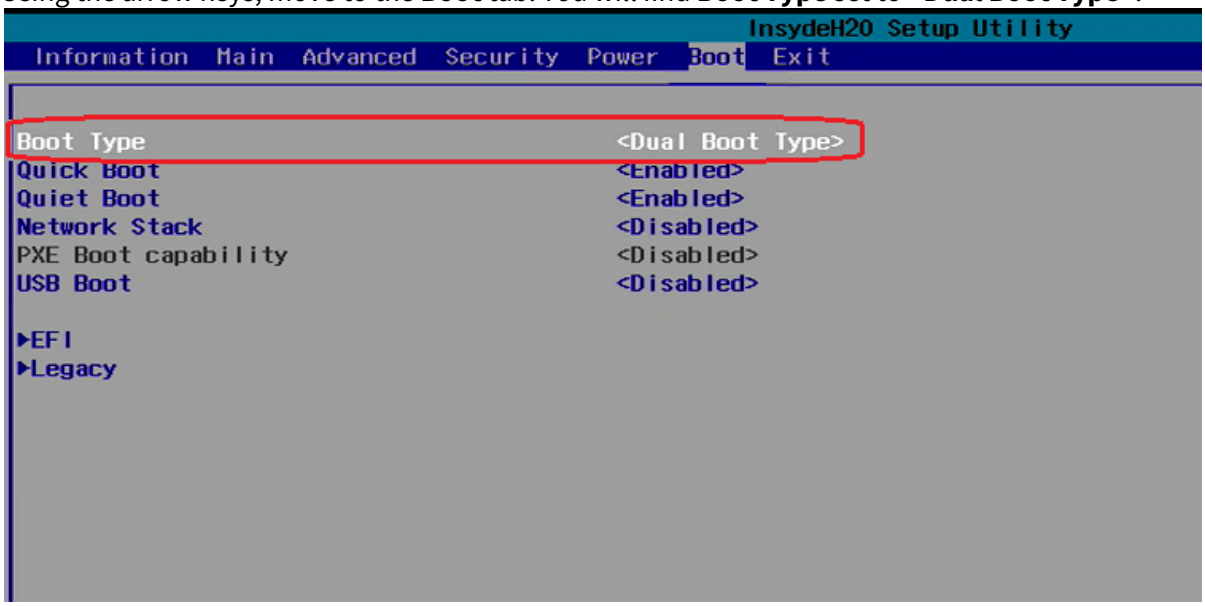
> To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *BayTrail.5.04.32.0022* or higher.

> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

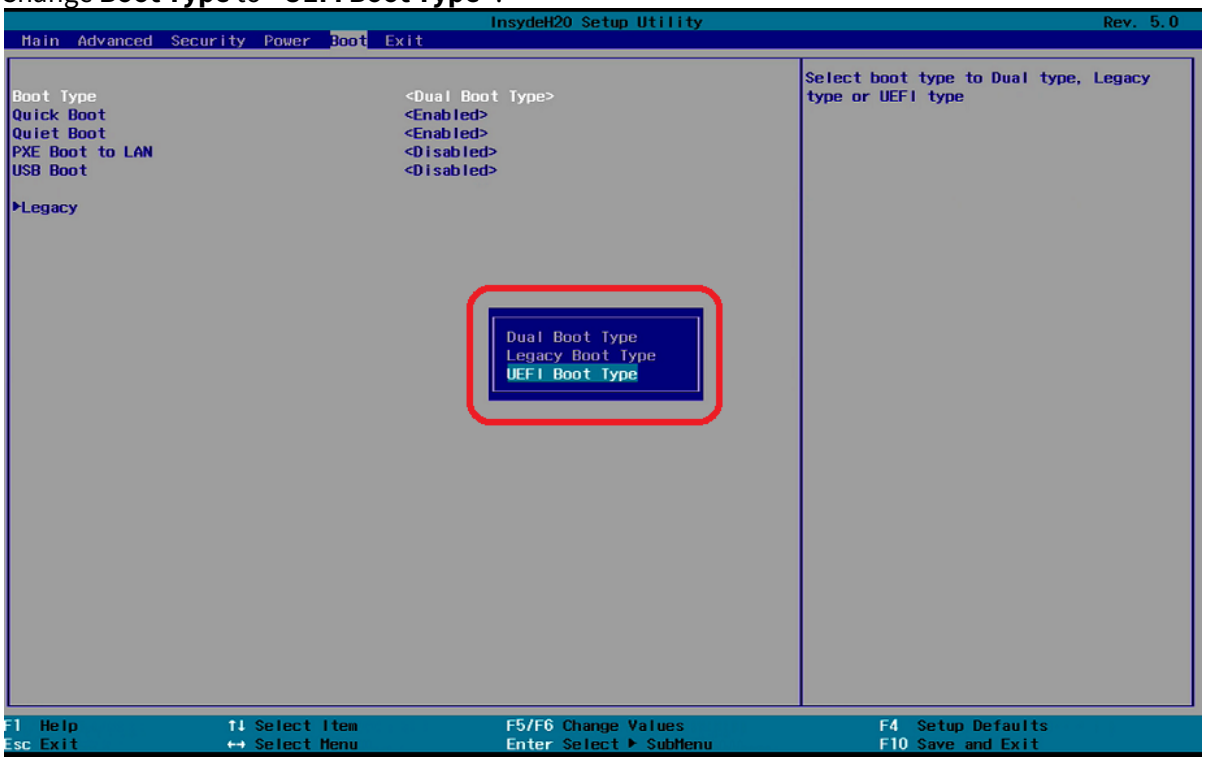
Changing the Device's Boot Type to UEFI Boot

1. Turn on (or restart) the IGEL device.
2. During boot, hold the [F2] key until you see the menu shown below.
3. Using the arrow keys, move to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.

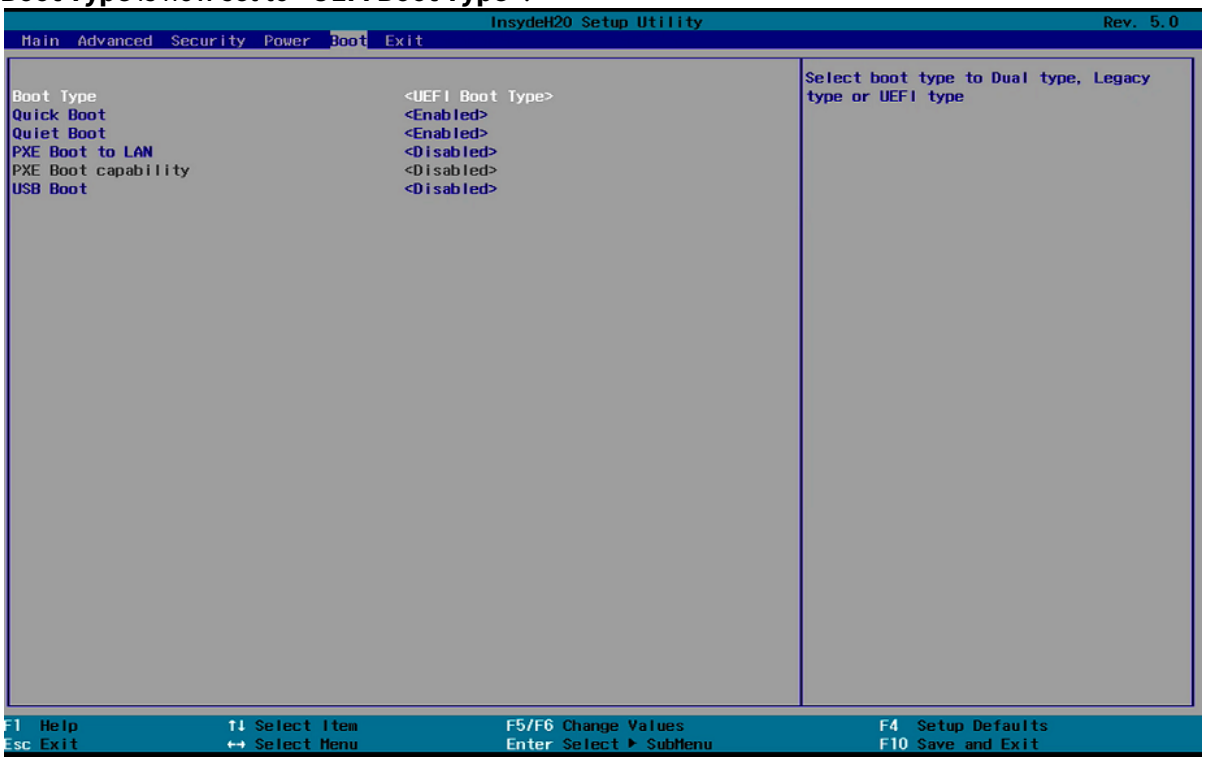
4. Using the arrow keys, move to the **Boot** tab. You will find **Boot Type** set to **<Dual Boot Type>**.



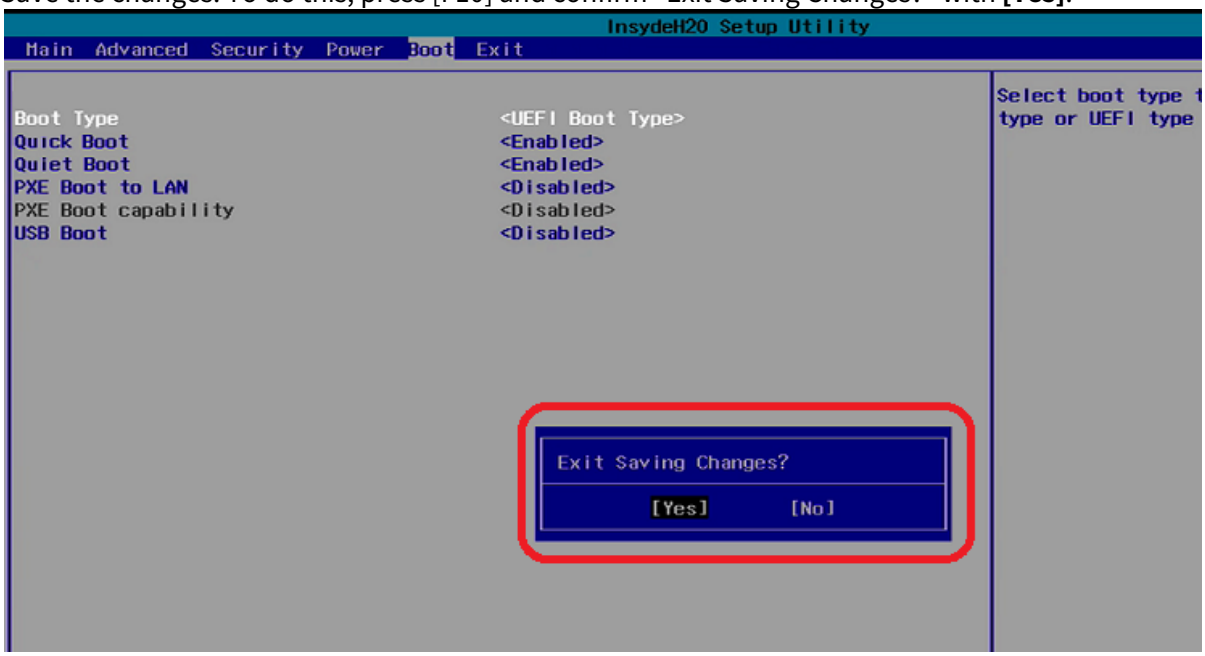
5. Change **Boot Type** to **<UEFI Boot Type>**.



Boot Type is now set to **<UEFI Boot Type>**.



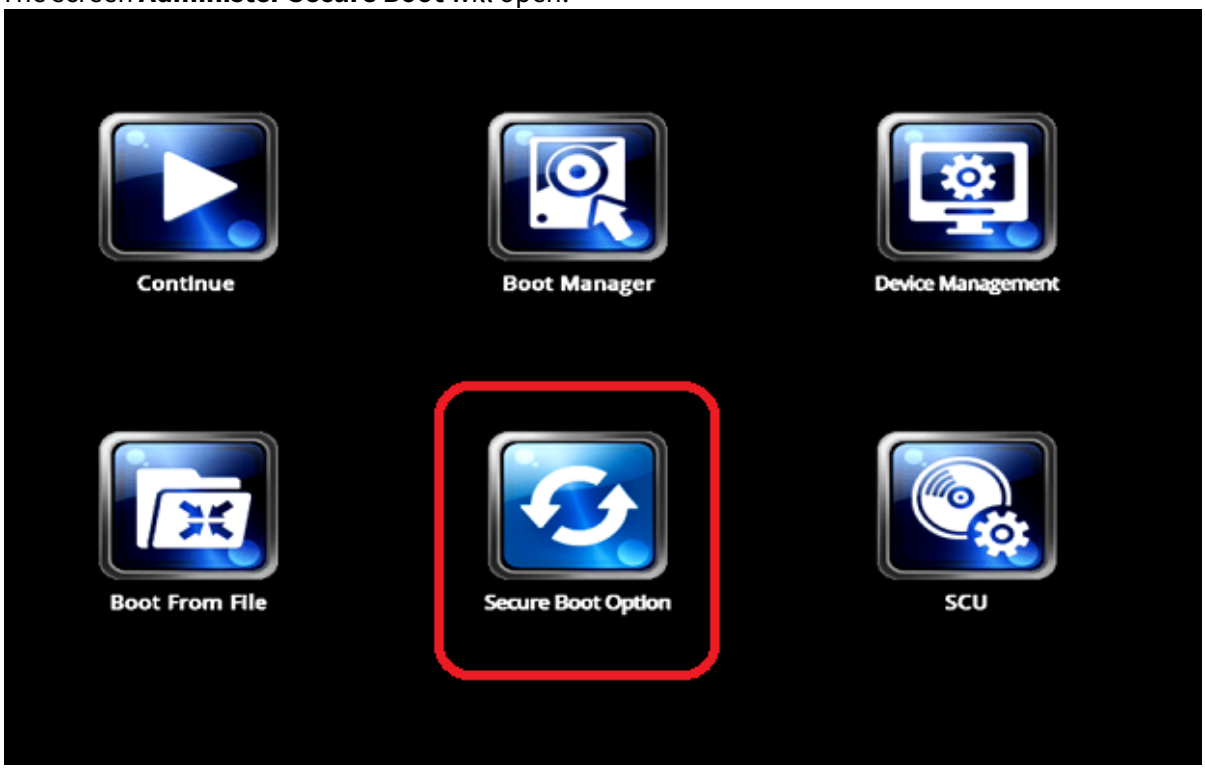
6. Save the changes. To do this, press [F10] and confirm "Exit Saving Changes?" with **[Yes]**.



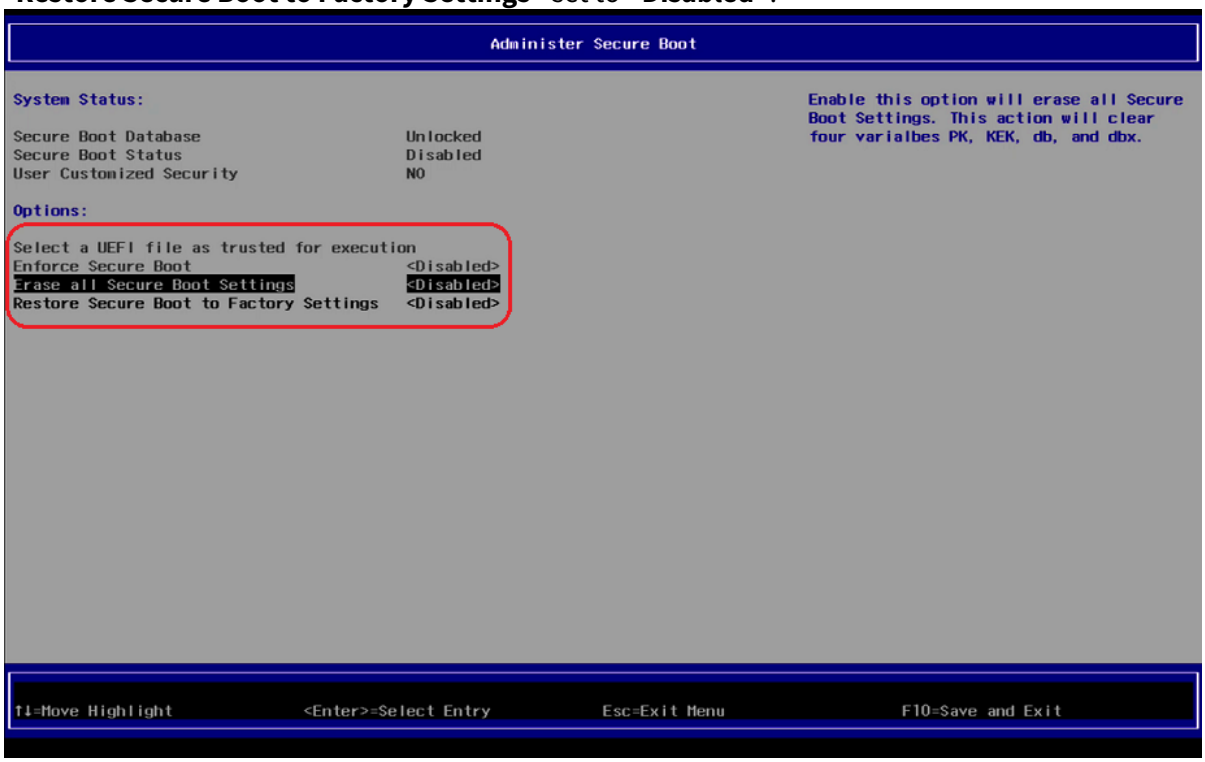
The settings are now saved and the device is rebooted.

Activating the Secure Boot Feature

1. Turn on (or restart) the IGEL device.
2. During boot, hold the [F2] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **Secure Boot Option** and press [ENTER].
   The screen **Administer Secure Boot** will open.

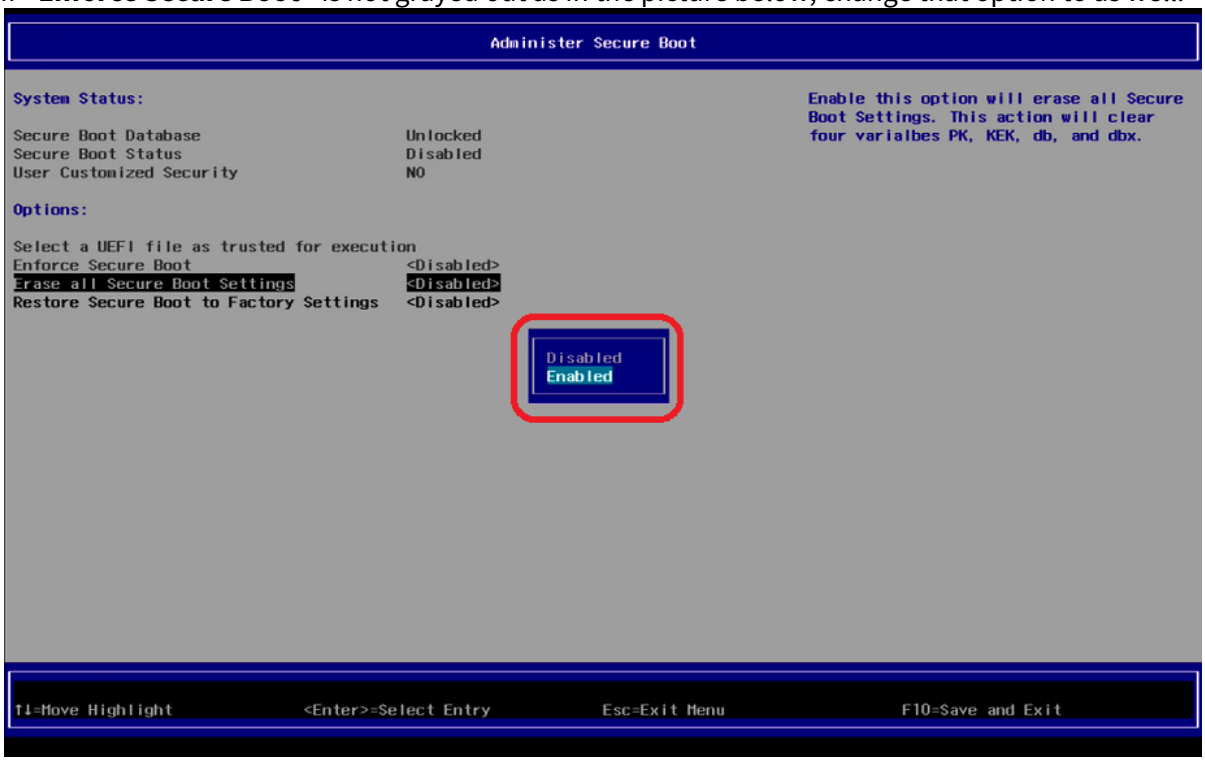


4. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.

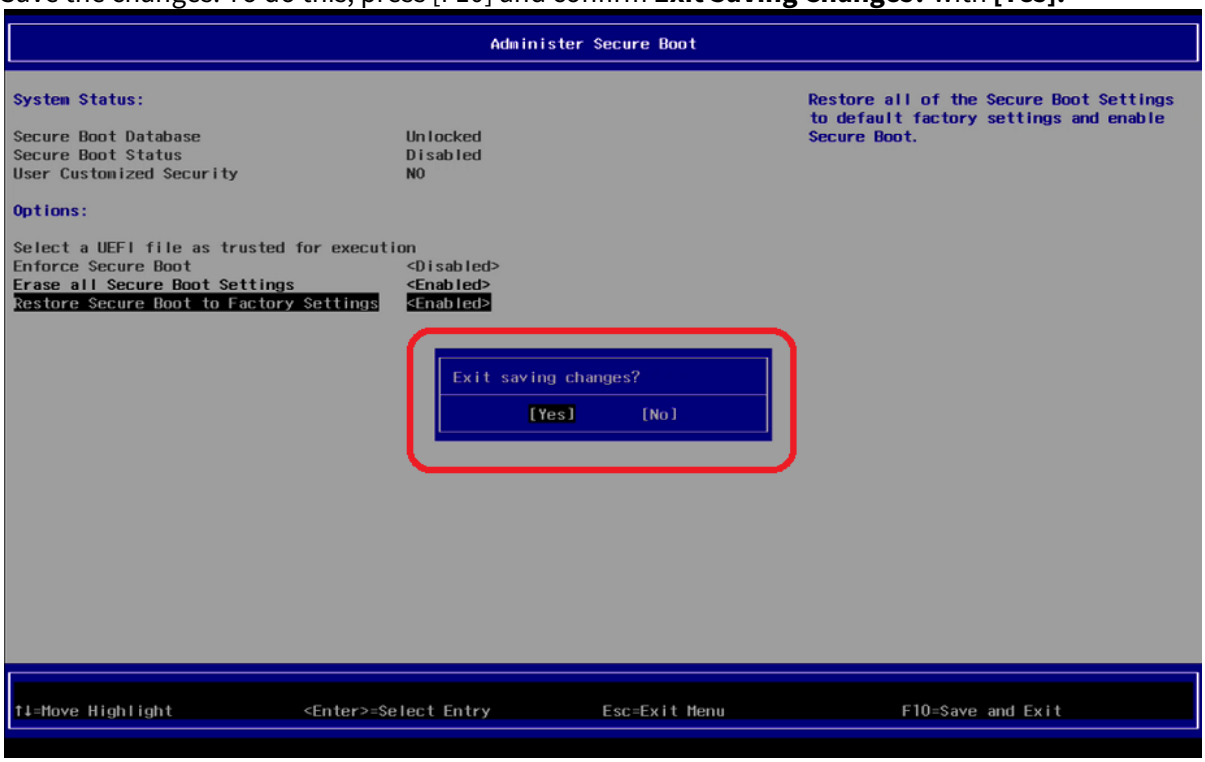


5. Change **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.

If **"Enforce Secure Boot"** is not grayed out as in the picture below, change that option to as well.



6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes].**



The changes are now saved and the device is rebooted.

7. As a last step, verify that Secure Boot is working, see Veryfing that UEFI Secure Boot is enabled.

Enabling UEFI Secure Boot in UD2-LX 50/51

UEFI Secure Boot is already a default setting in UD2-LX 50 and UD2-LX 51.

If you have disabled secure boot, you will need to reverse the settings you made.

Enabling UEFI Secure Boot in UD3-LX 50

Prerequisites

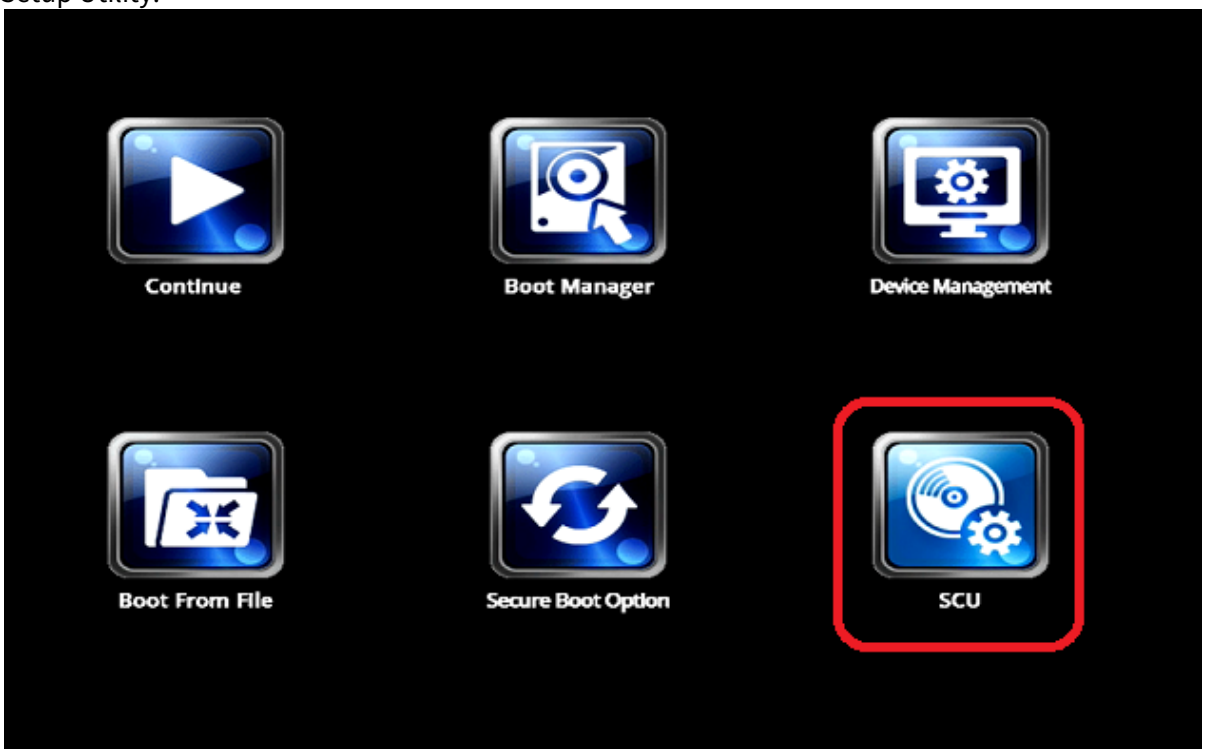
- IGEL OS 10.04.100 or higher
- BIOS version 3.A. 13-11202017 or higher

> To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *3.A. 13-11202017* or higher.

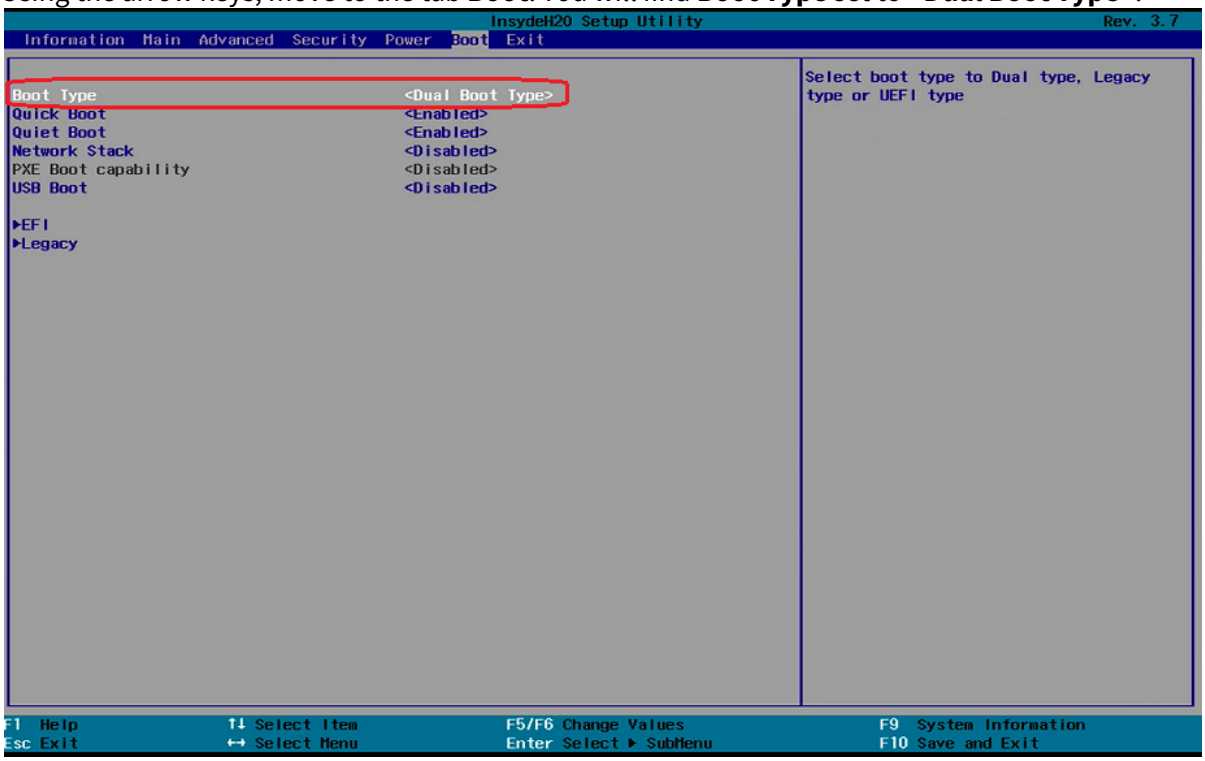
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Changing the Device's Boot Type to UEFI Boot

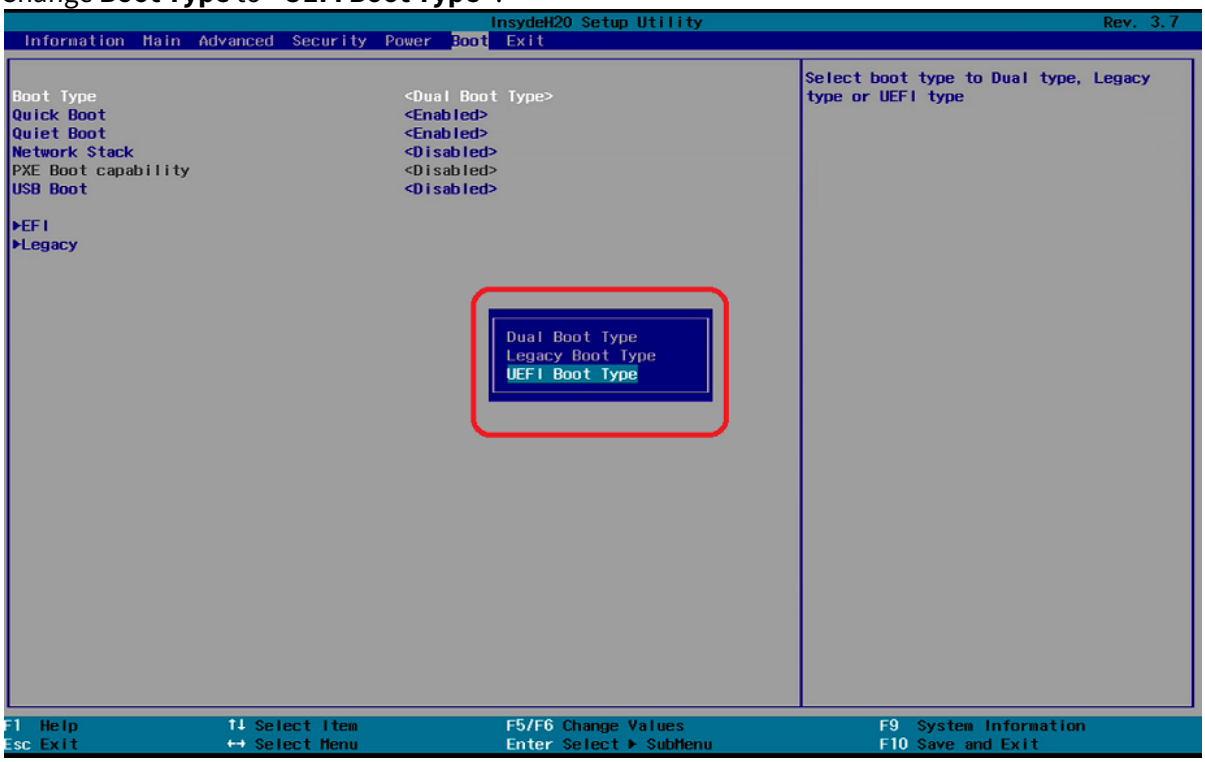
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



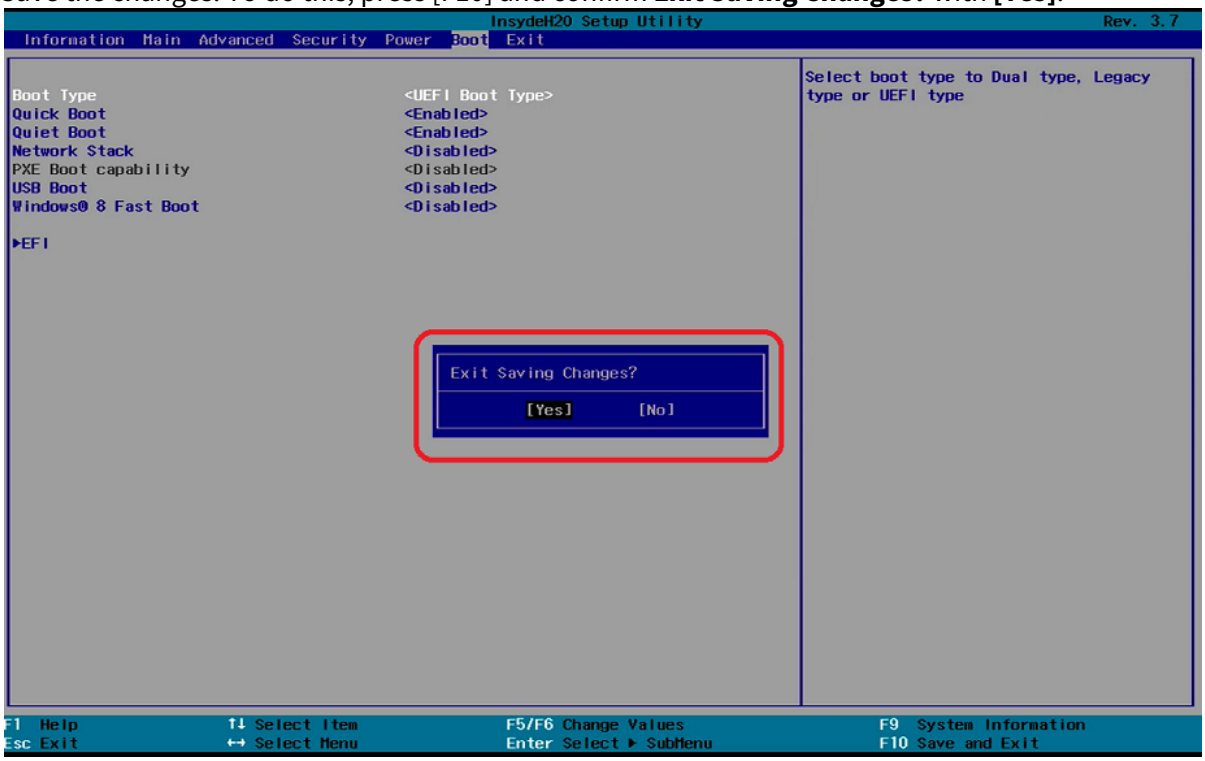
4. Using the arrow keys, move to the tab **Boot**. You will find **Boot Type** set to **<Dual Boot Type>**.



5. Change **Boot Type** to **<UEFI Boot Type>**.



6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.

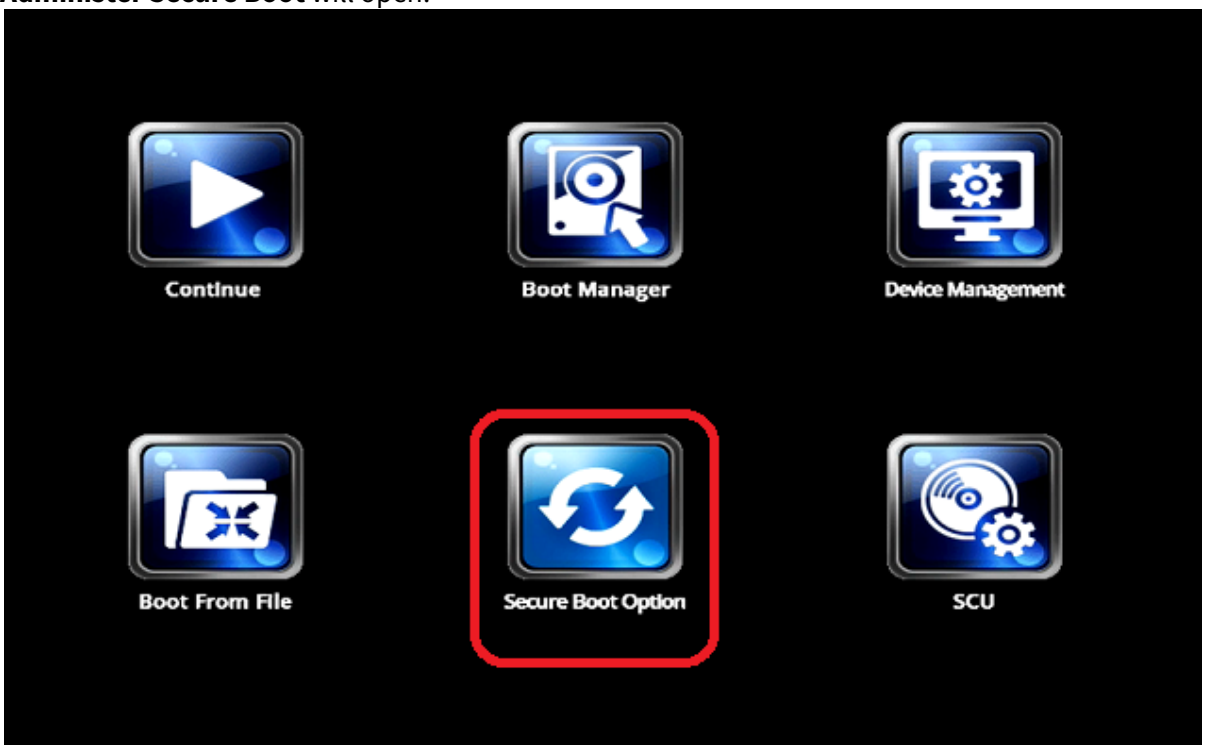


The changes will be saved and the device will be rebooted.

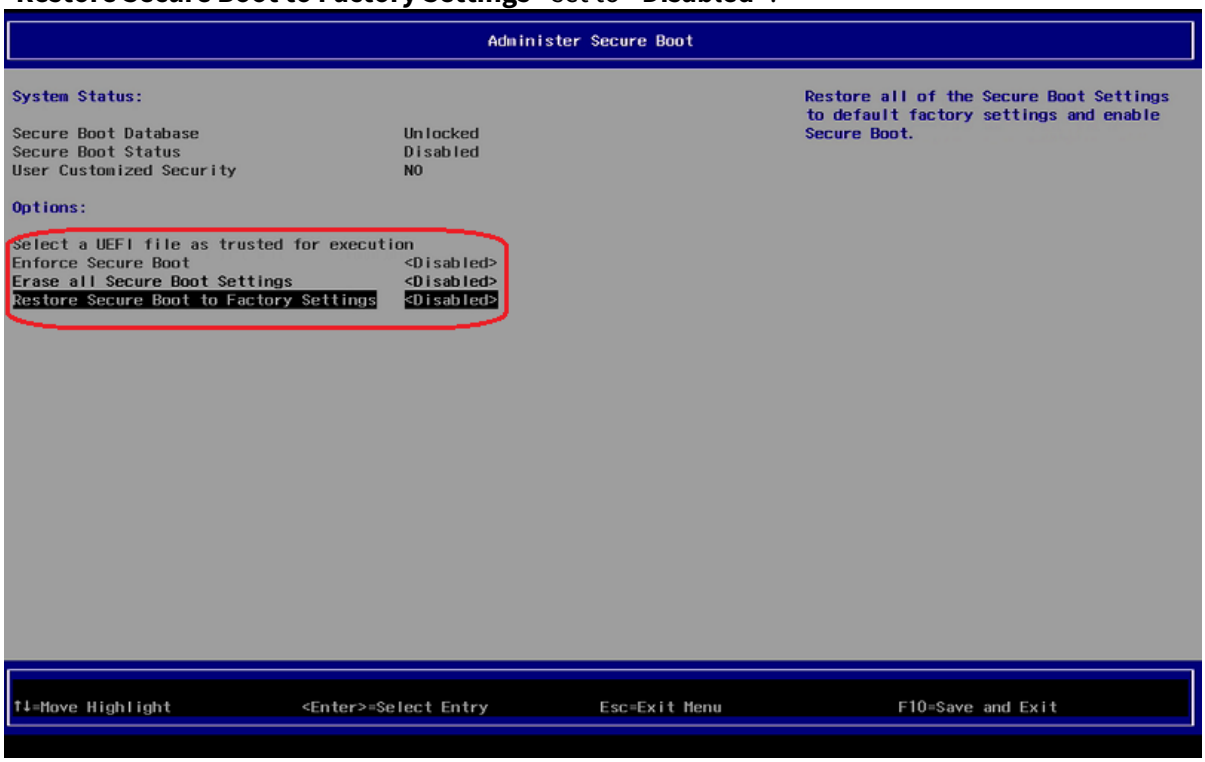
Activating the Secure Boot Feature

1. Turn on (or restart) the IGEL device.

2. Using the arrow keys, move to **Secure Boot Option** and press [ENTER]. The BIOS screen **Administer Secure Boot** will open.

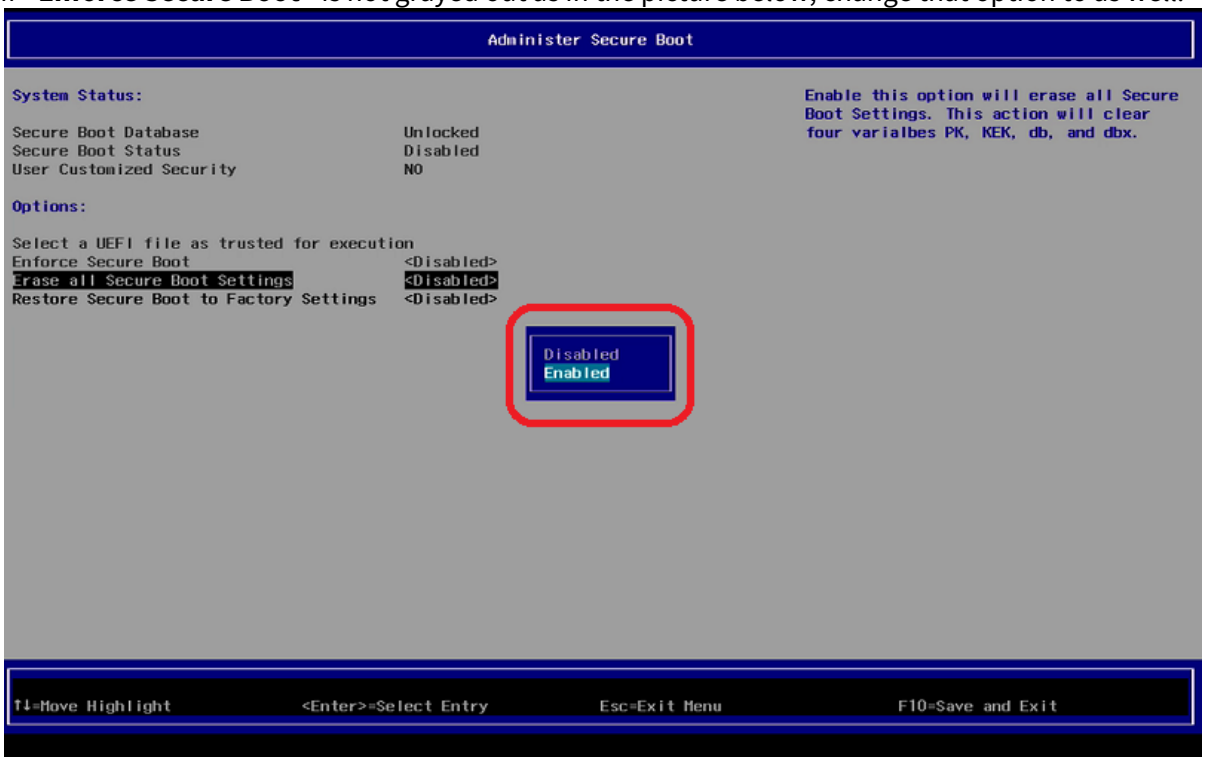


3. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.

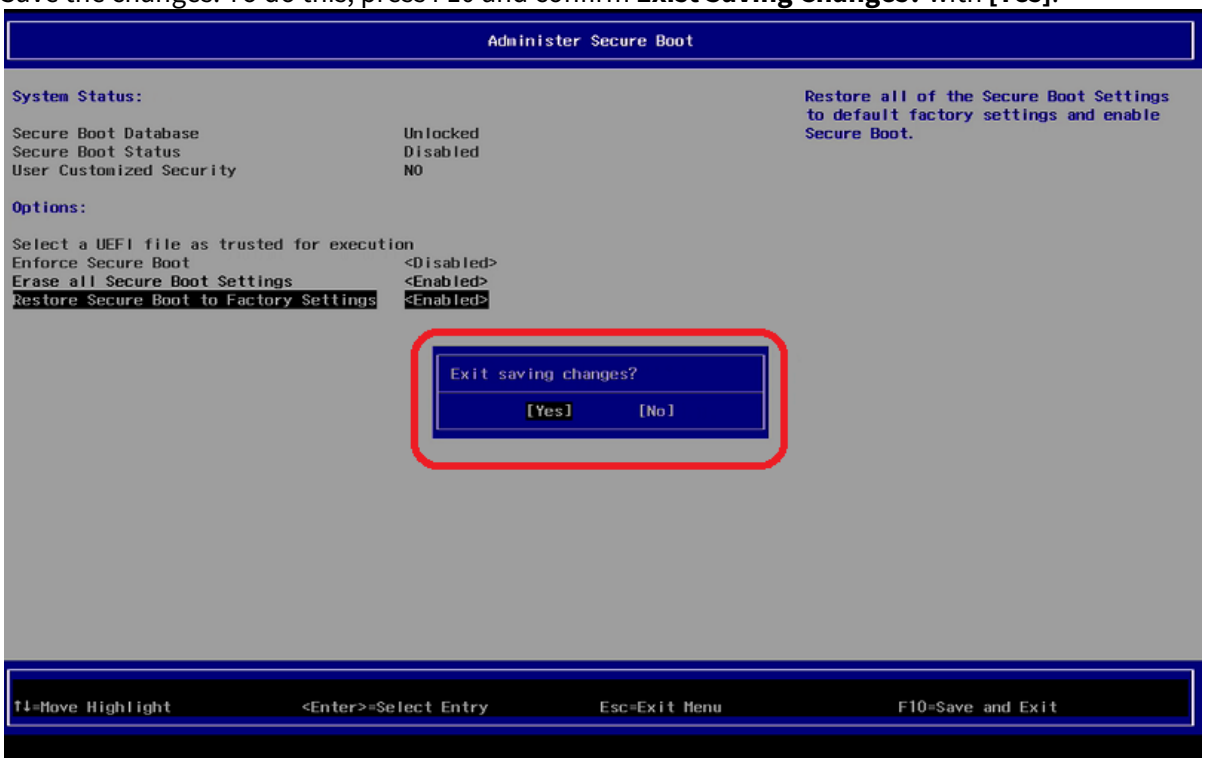


4. Change **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.

If **"Enforce Secure Boot"** is not grayed out as in the picture below, change that option to as well.



5. Save the changes. To do this, press F10 and confirm **Exist Saving Changes?** with **[Yes]**.



The changes will be saved and the device will be rebooted.

6. As a last step, verify that Secure Boot is working, see Veryfing that UEFI Secure Boot is enabled.

Enabling UEFI Secure Boot in UD3-LX 51

Prerequisites

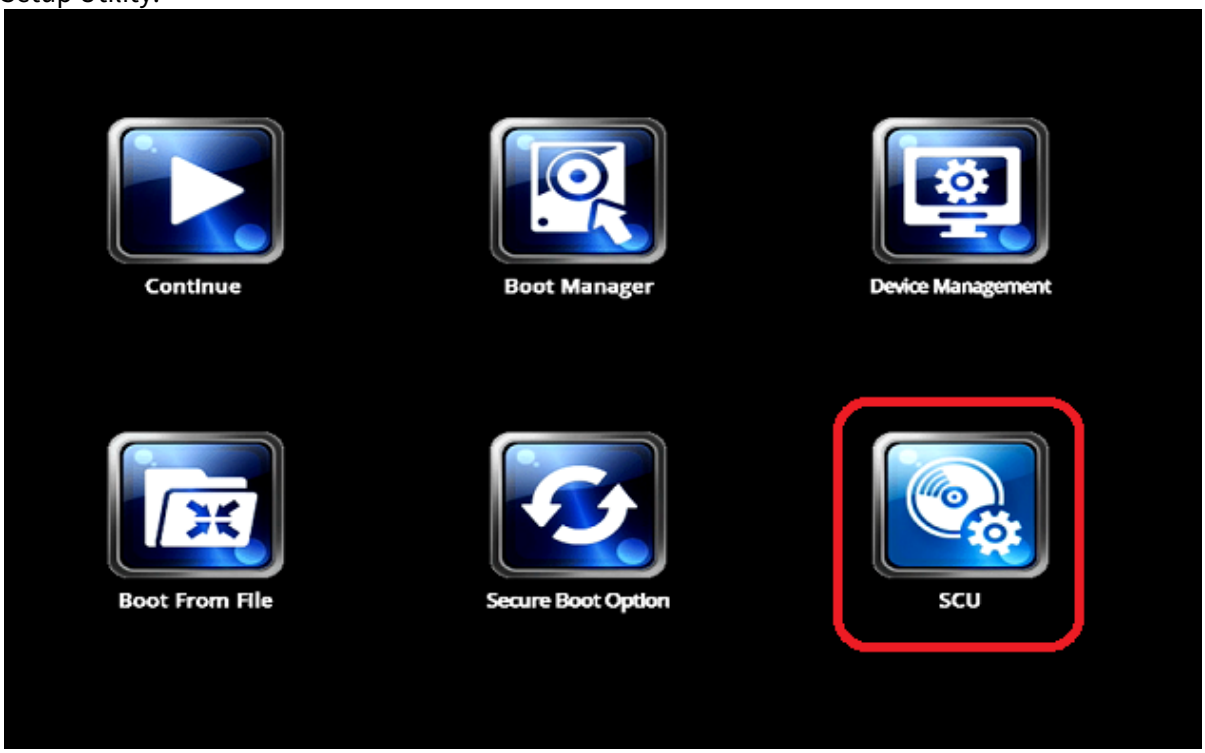
- IGEL OS 10.04.100 or higher
- BIOS version 3.A. 13-11202017 or higher

> To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *3.A. 13-11202017* or higher.

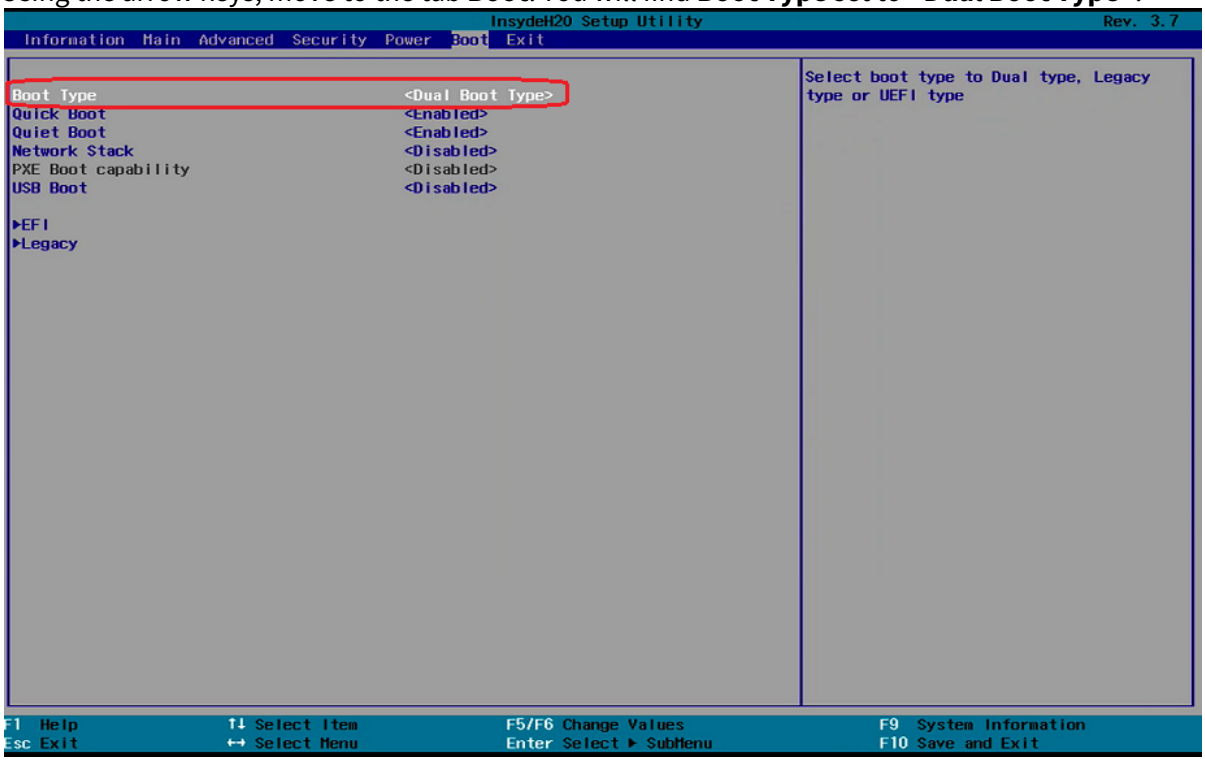
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Changing the Device's Boot Type to UEFI Boot

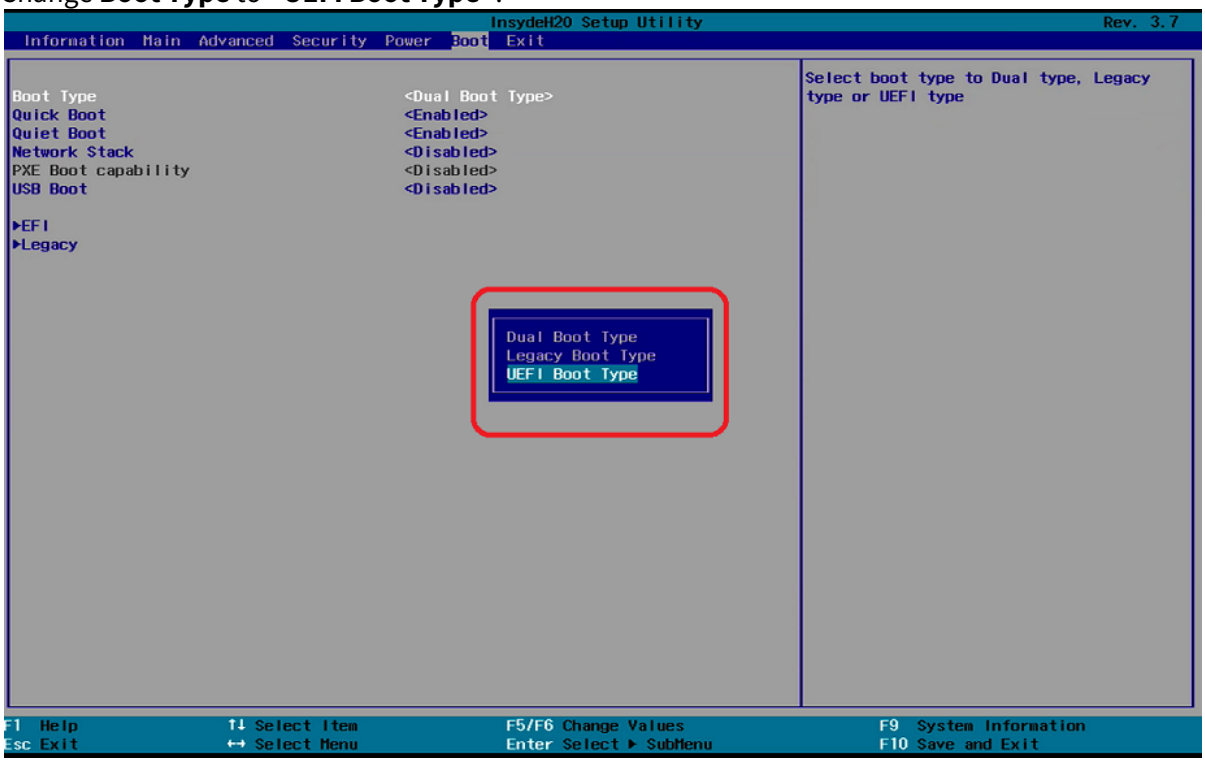
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



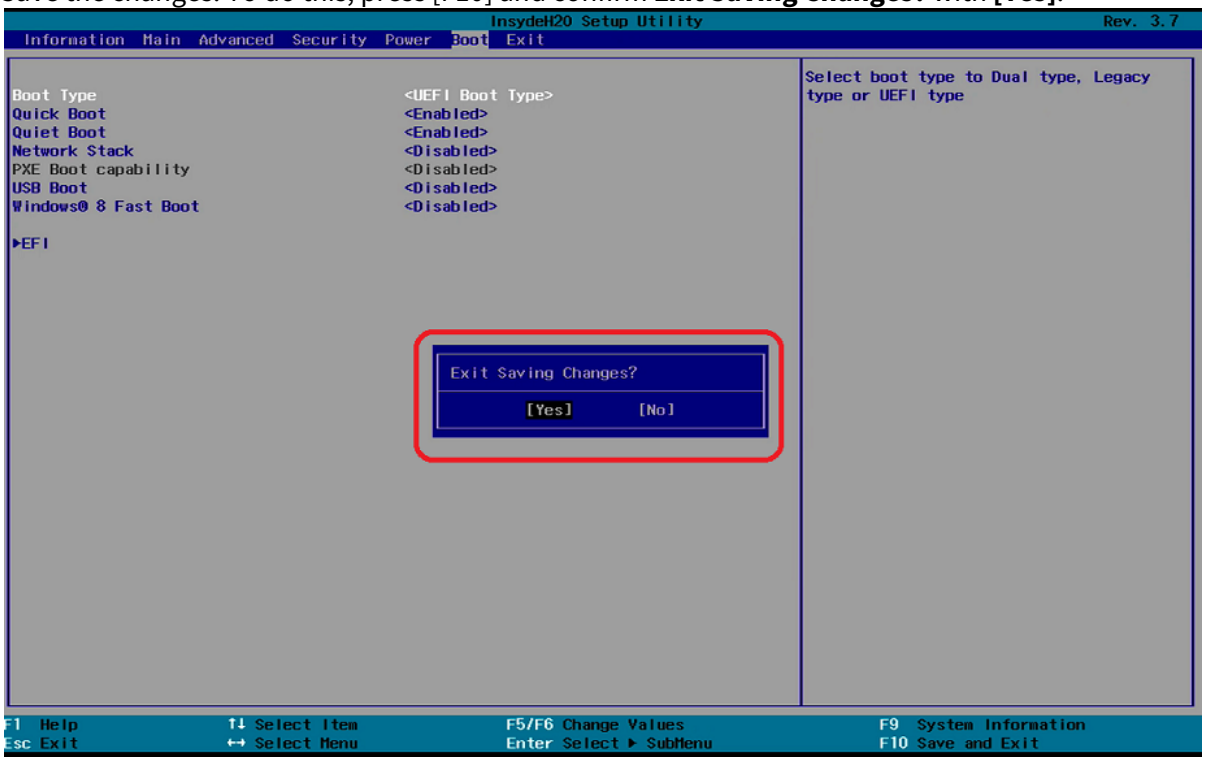
4. Using the arrow keys, move to the tab **Boot**. You will find **Boot Type** set to **<Dual Boot Type>**.



5. Change **Boot Type** to **<UEFI Boot Type>**.



6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.

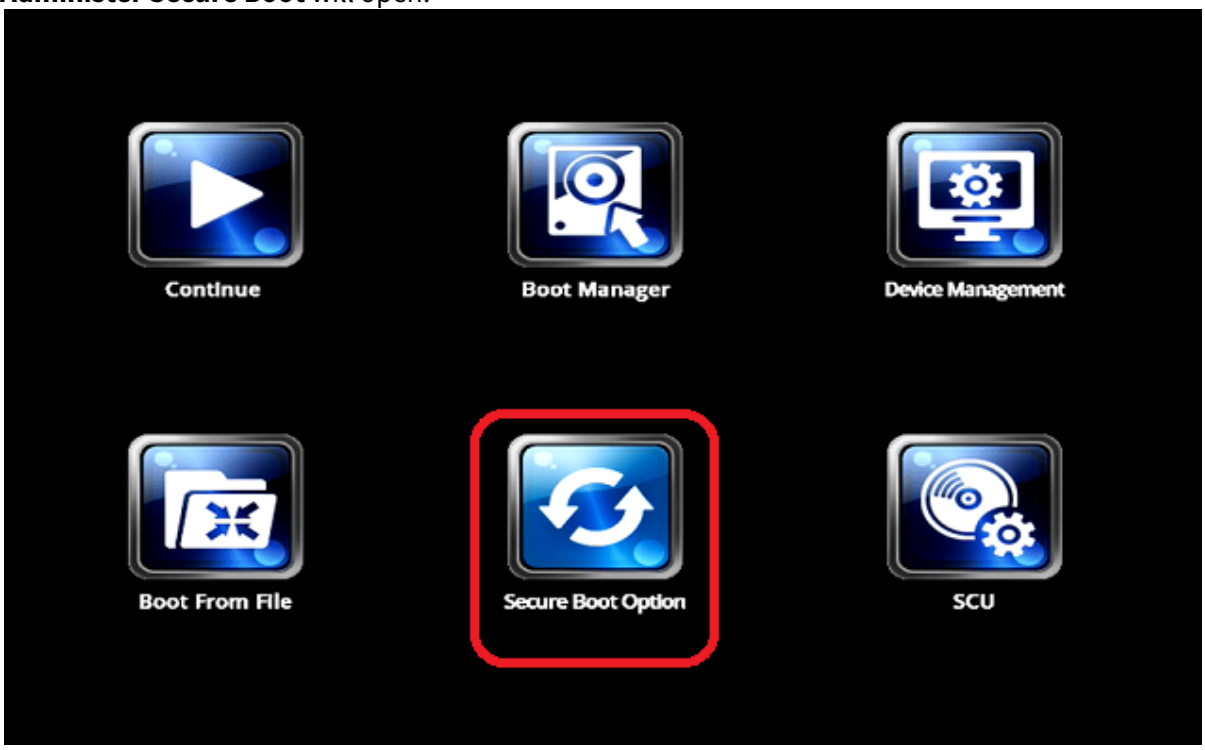


The changes will be saved and the device will be rebooted.

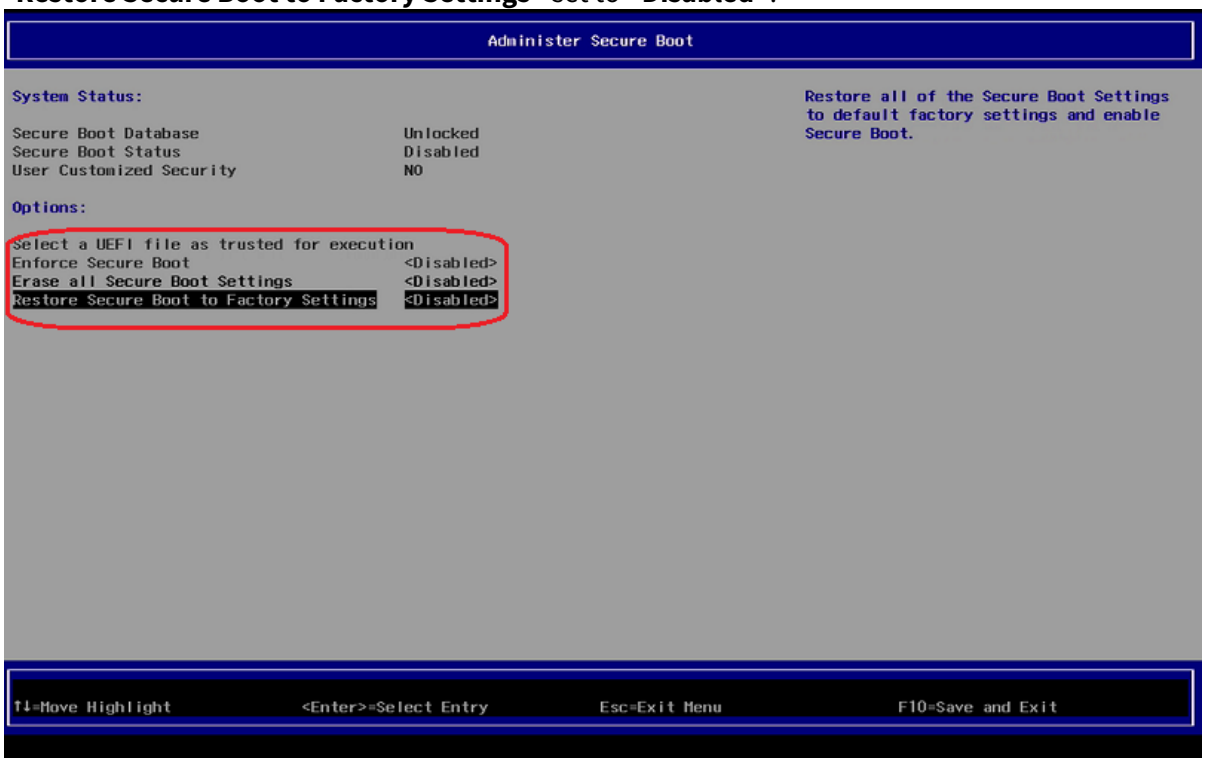
Activating the Secure Boot Feature

1. Turn on (or restart) the IGEL device.

2. Using the arrow keys, move to **Secure Boot Option** and press [ENTER]. The BIOS screen **Administer Secure Boot** will open.

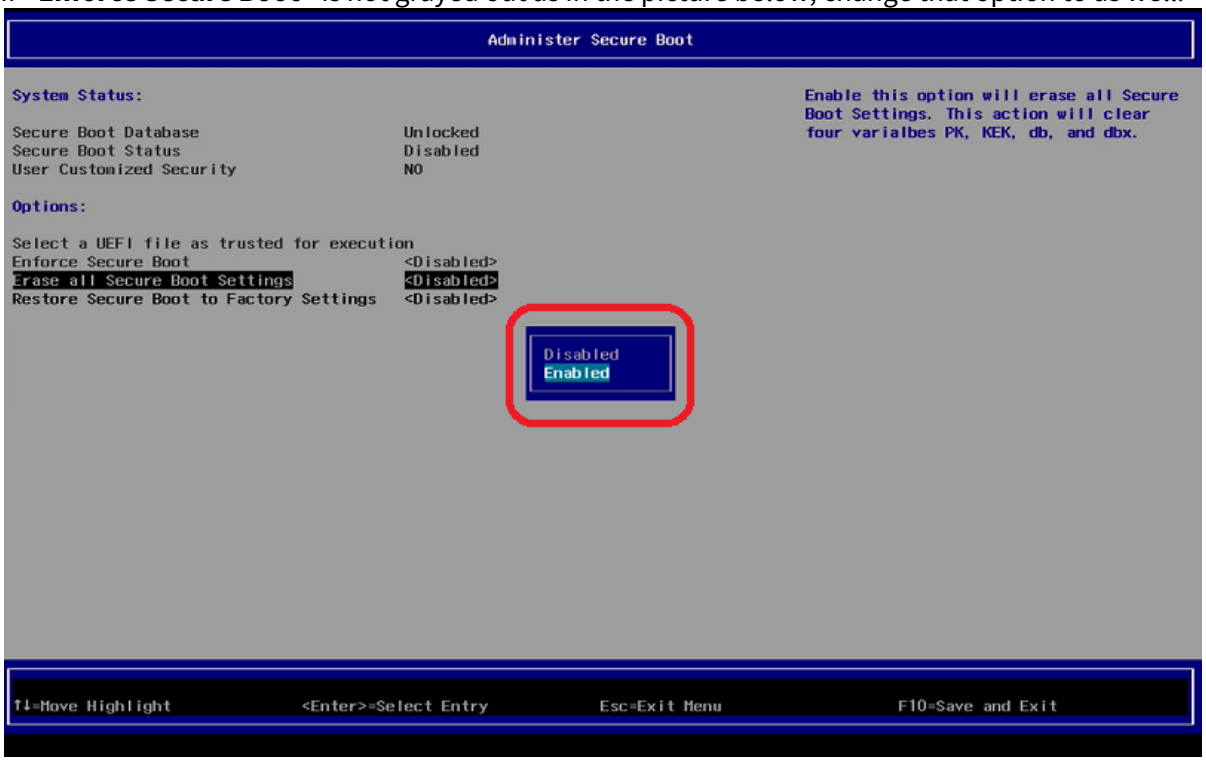


3. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.

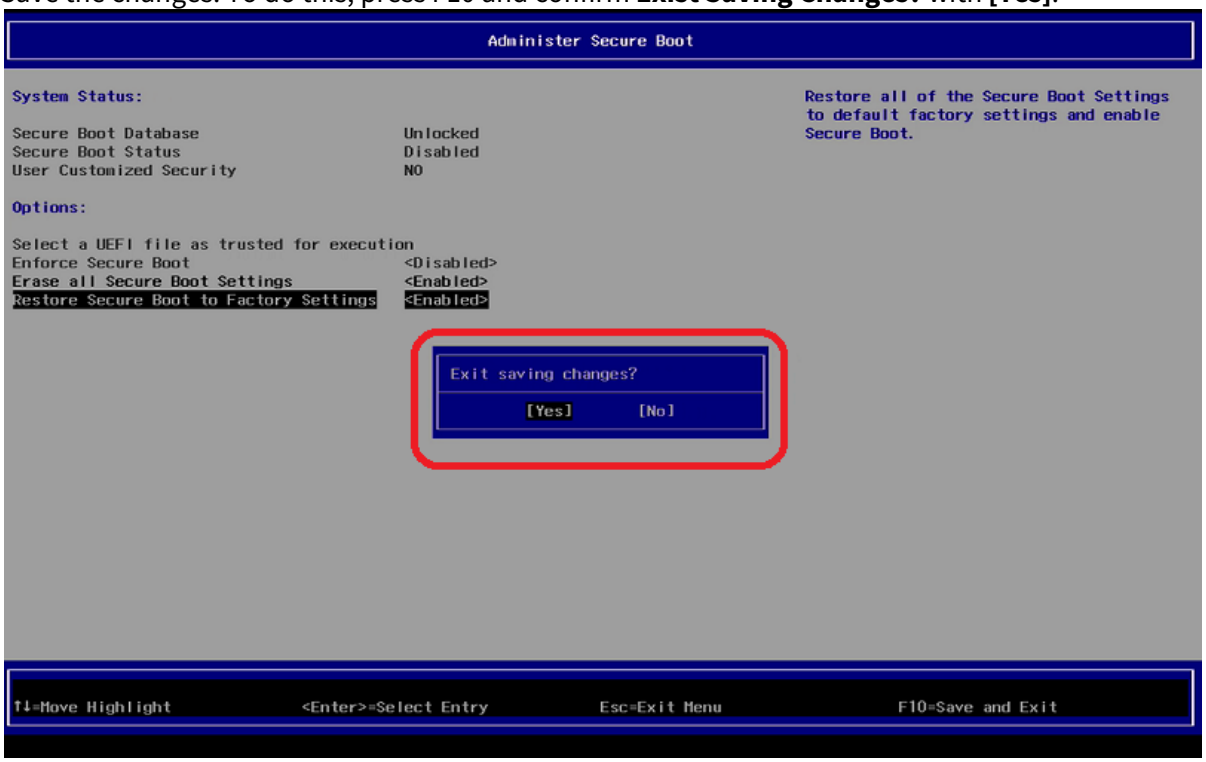


4. Change **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.

If **"Enforce Secure Boot"** is not grayed out as in the picture below, change that option to as well.



5. Save the changes. To do this, press F10 and confirm **Exist Saving Changes?** with **[Yes]**.



The changes will be saved and the device will be rebooted.

6. As a last step, verify that Secure Boot is working, see Veryfing that UEFI Secure Boot is enabled.

Enabling UEFI Secure Boot in UD3-LX 60

UEFI Secure Boot is already a default setting in UD3-LX 60.

If you have disabled secure boot, you will need to reverse the settings you made.

Enabling UEFI Secure Boot in UD6-LX 51

Prerequisites

- IGEL OS 10.04.100 or higher

> The version of IGEL OS can be found in the About window.

- BIOS version 3.9. 13-02202017 or higher

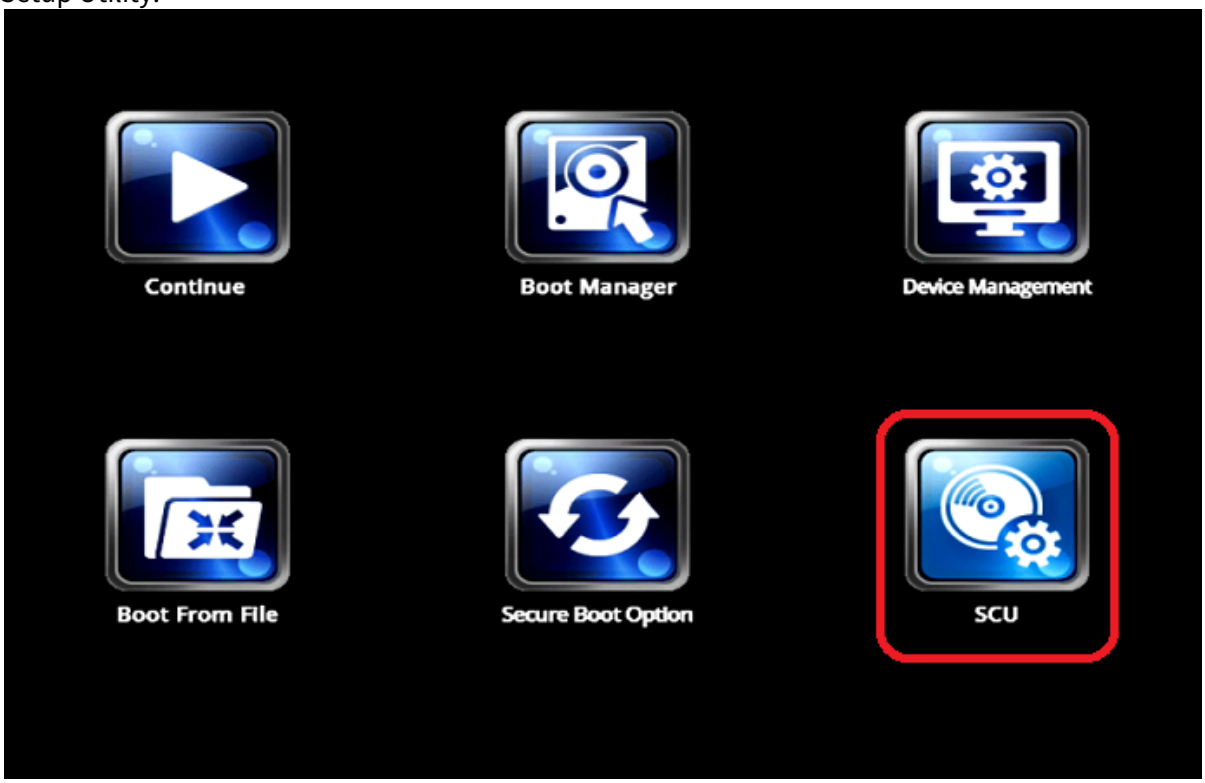
> To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *3.9. 13-02202017* or newer.

> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

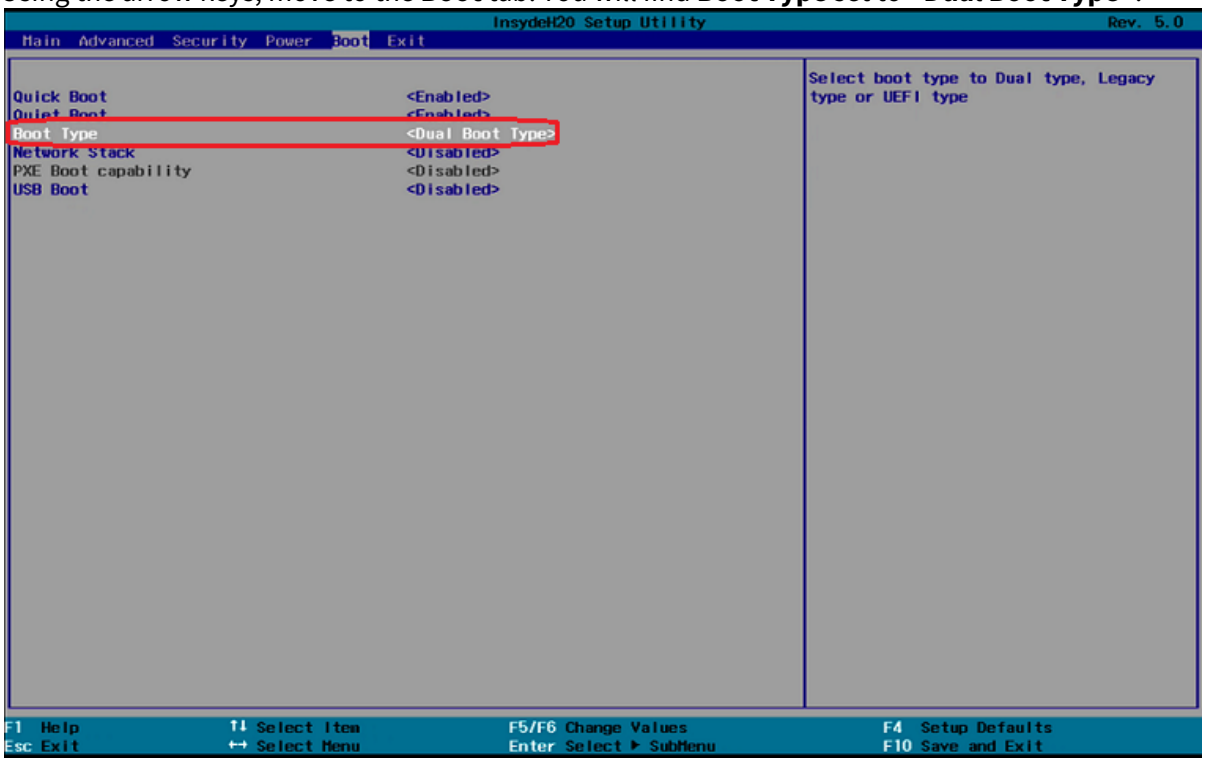
Changing the Device's Boot Type to UEFI Boot

1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.

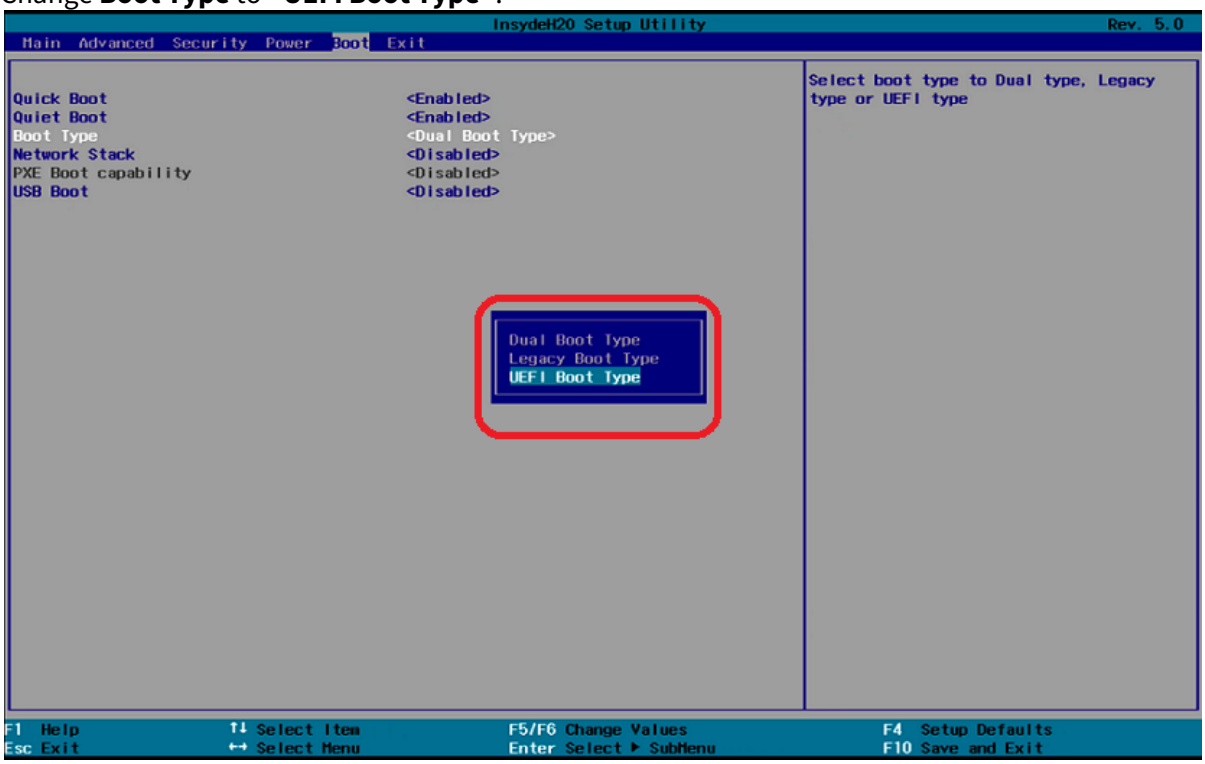
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



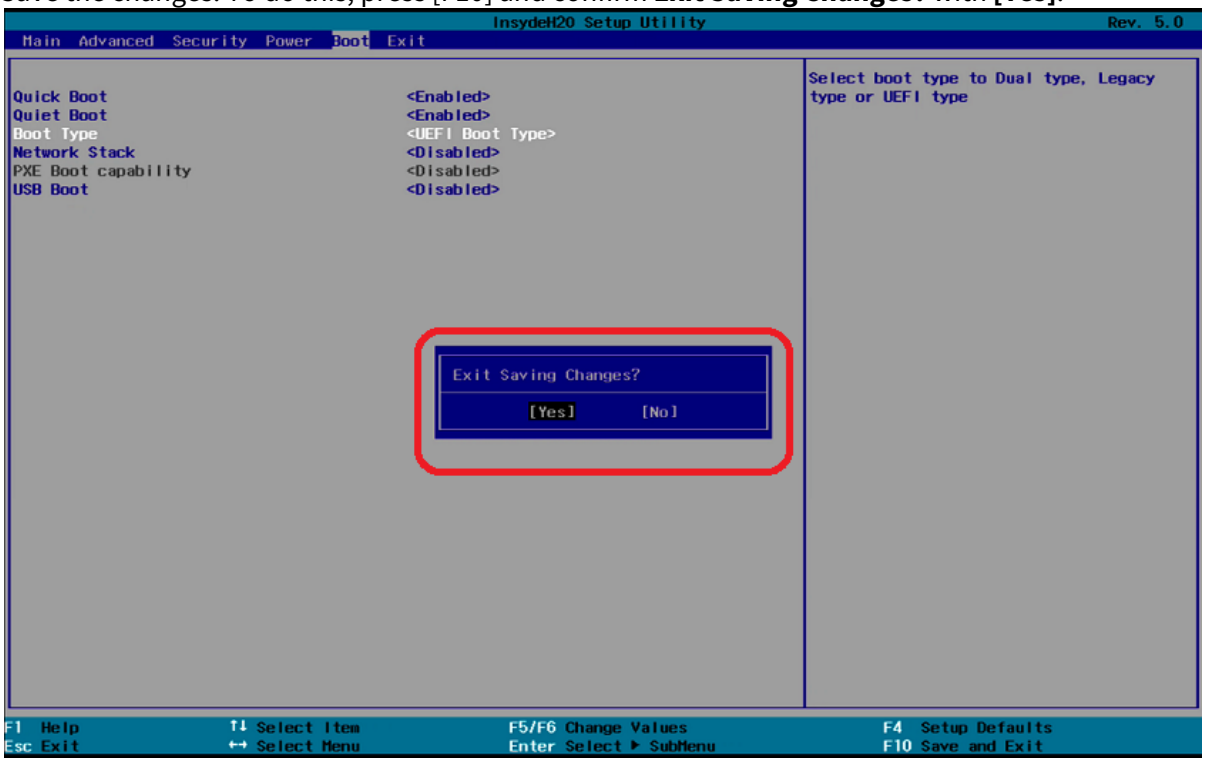
4. Using the arrow keys, move to the **Boot** tab. You will find **Boot Type** set to **<Dual Boot Type>**.



5. Change **Boot Type** to **<UEFI Boot Type>**.



6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.

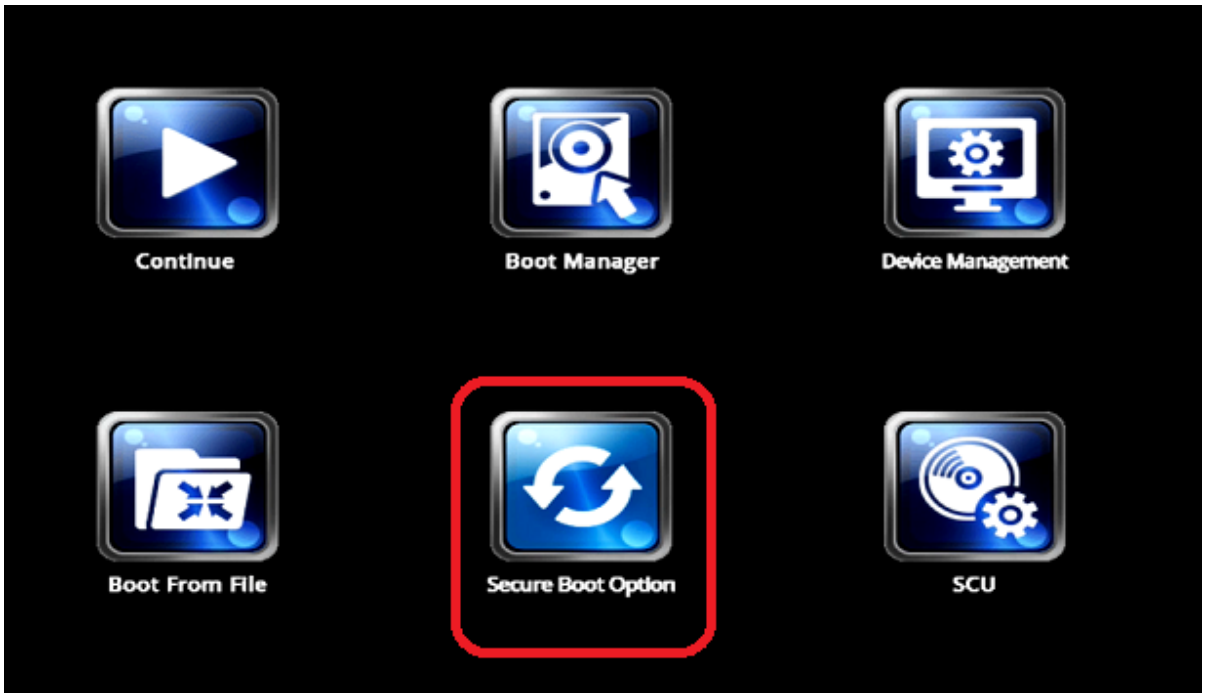


The changes will be saved and the device will be rebooted.

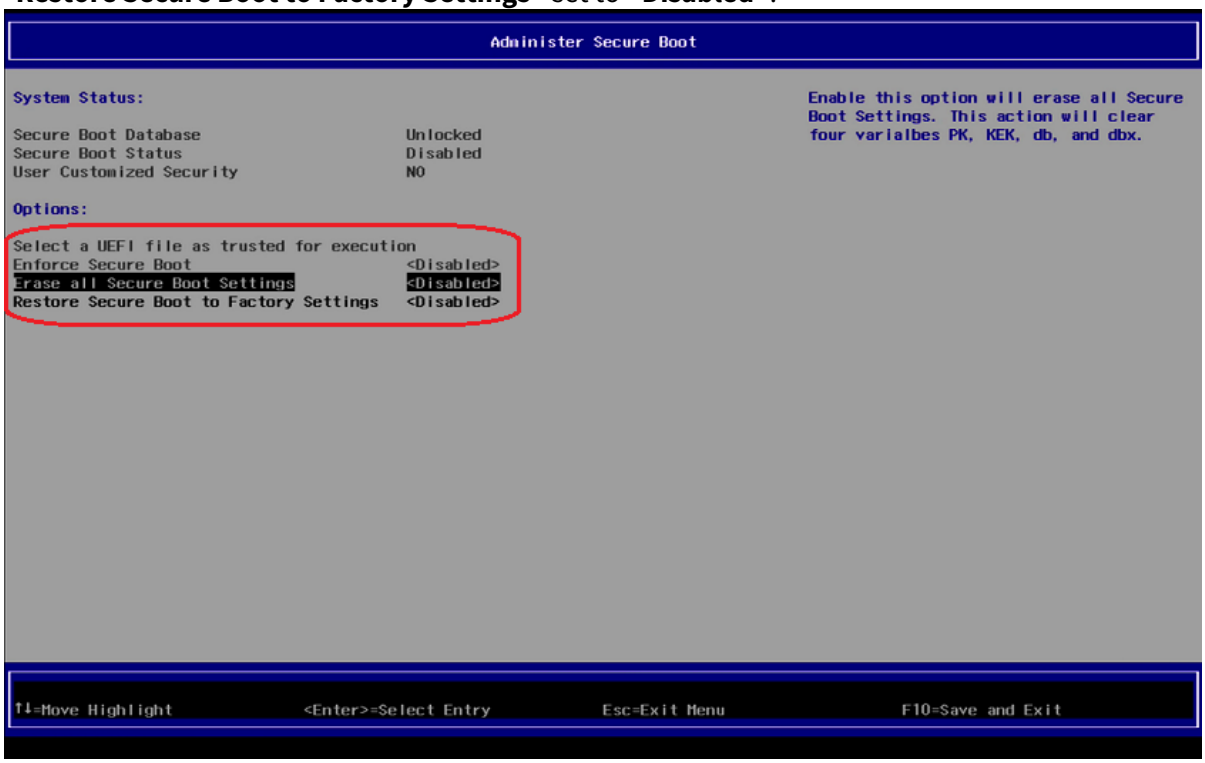
Activating the Secure Boot Feature

1. Turn on (or restart) the device.
2. During boot, hold the [DEL] key until you see the screen shown below.

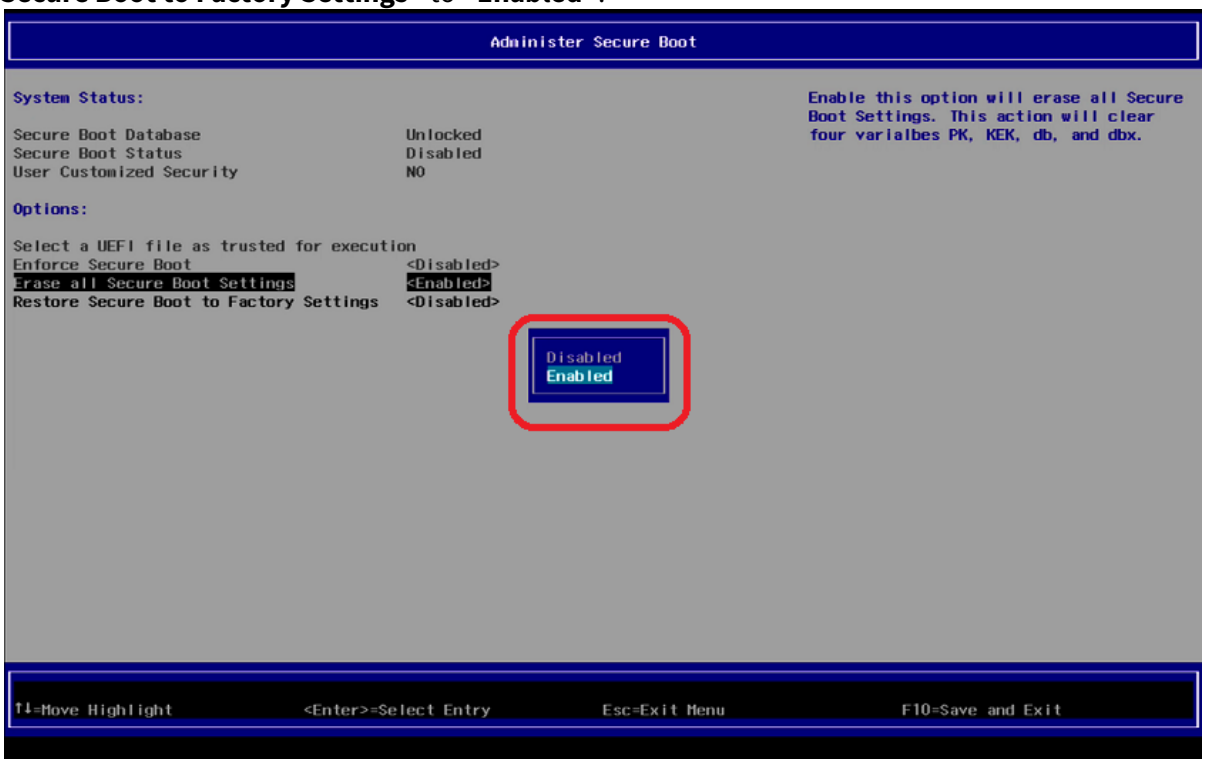
3. Using the arrow keys, move to the option **Secure Boot Option**, and press [ENTER]. This will open the the screen **Administer Secure Boot**.



4. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.

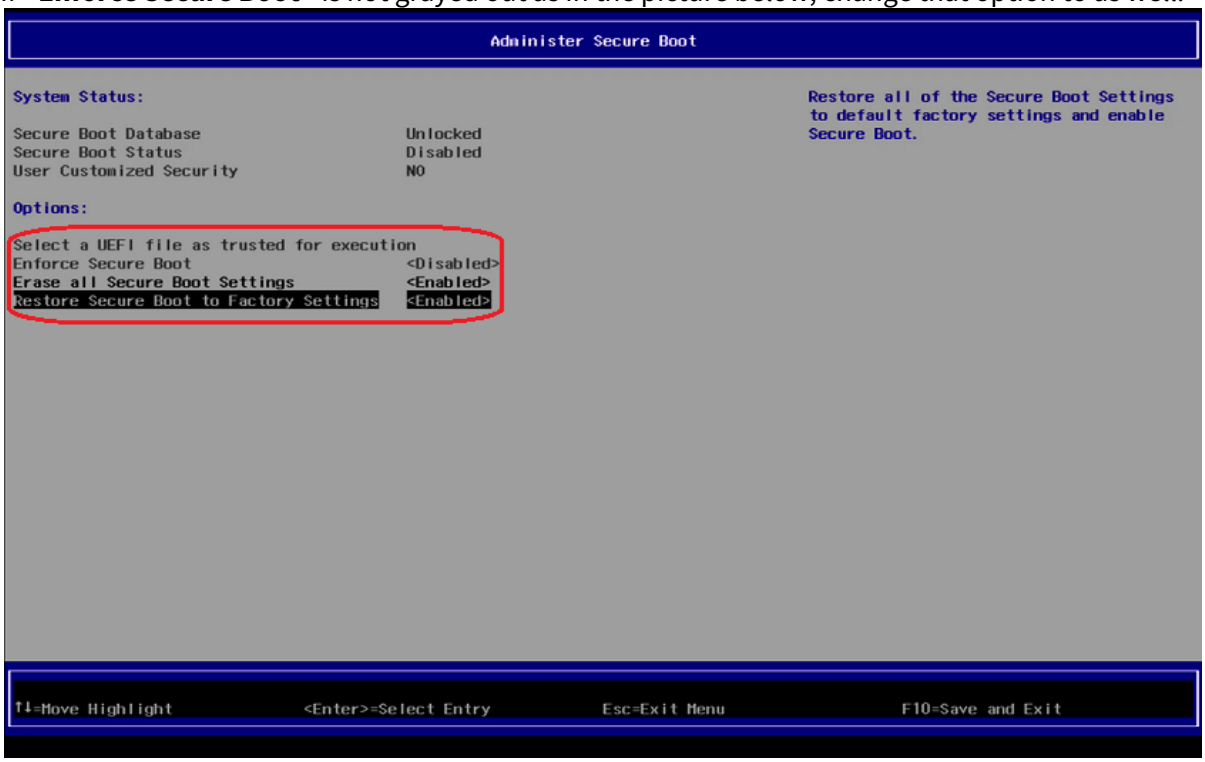


5. In the screen **Administer Secure Boot**, set "**Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.

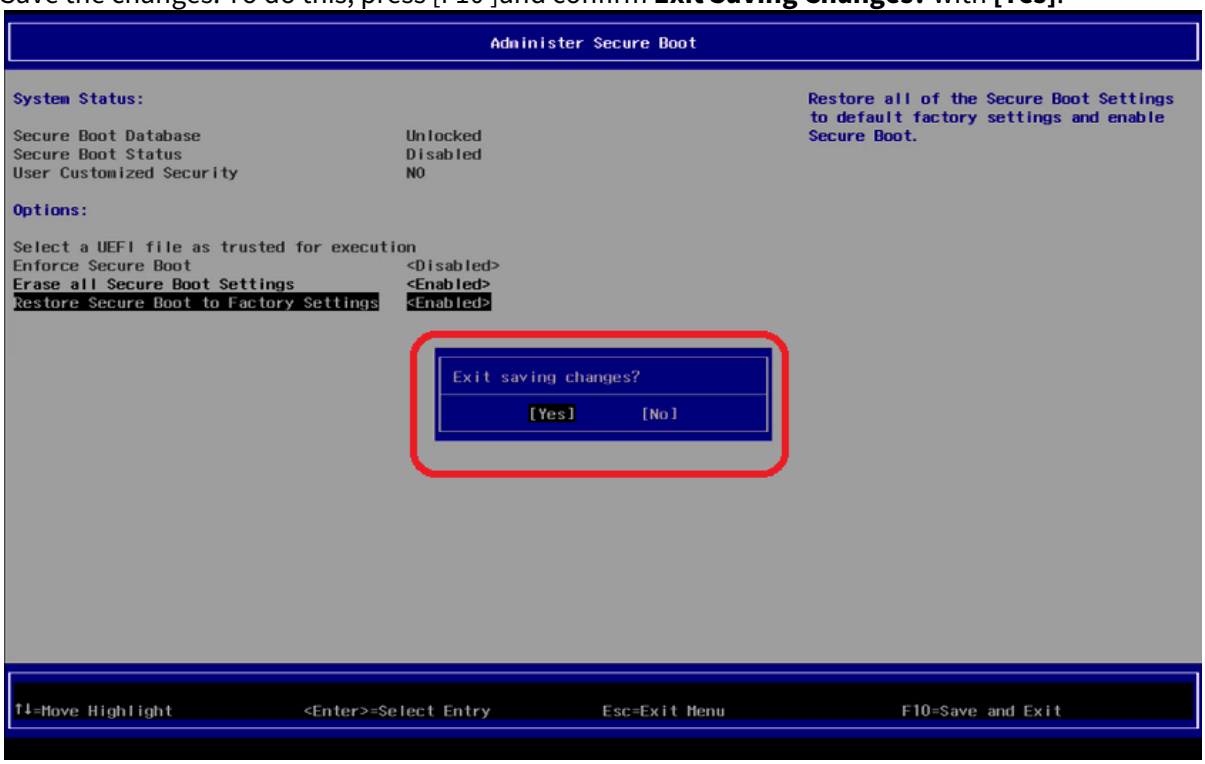


6. **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** are now set to **<Enabled>**.

If **"Enforce Secure Boot"** is not grayed out as in the picture below, change that option to as well.



7. Save the changes. To do this, press [F10]and confirm **Exit Saving Changes?** with **[Yes]**.



The changes will be saved and the device will be rebooted.

8. As a last step, verify that Secure Boot is working, see Veryfing that UEFI Secure Boot is enabled.

Enabling UEFI Secure Boot in UD7-LX 10

Prerequisites

- IGEL OS 10.04.100 or higher

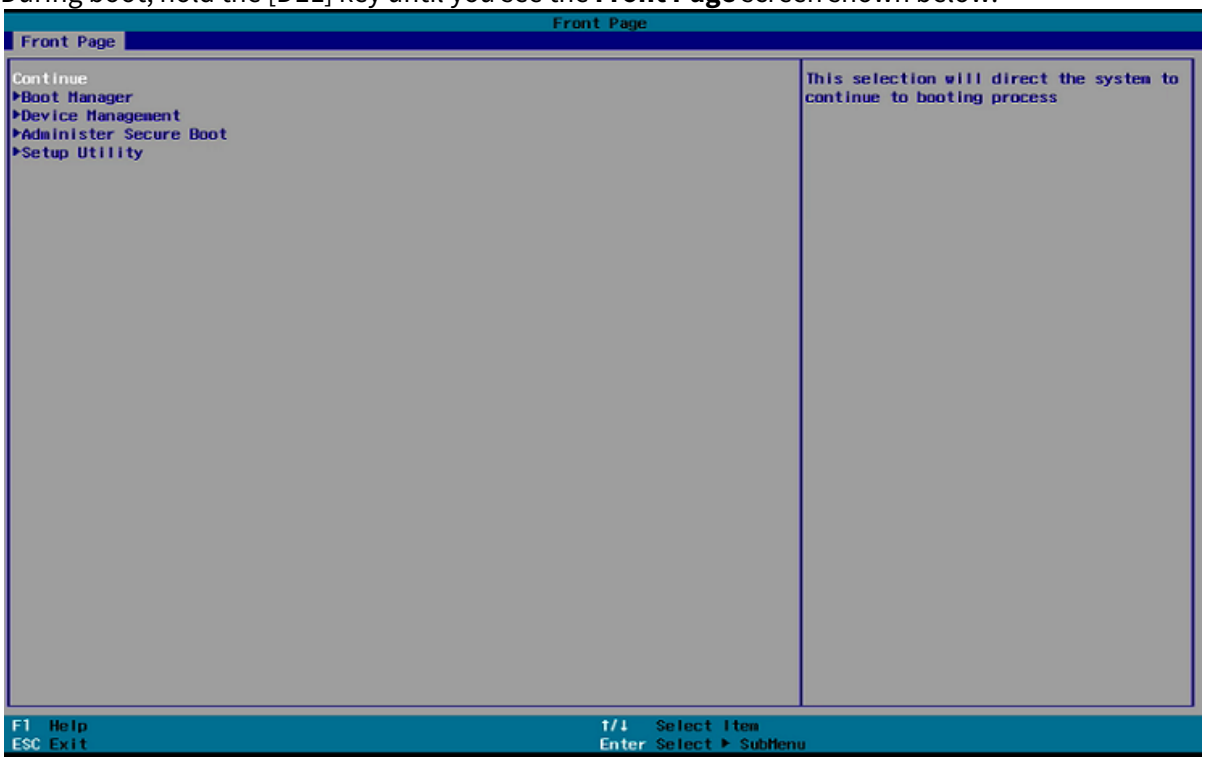
> The version of IGEL Linux can be found in the **About** window.

> UD7-LX 10 supports UEFI Secure Boot by default and no BIOS update is necessary.

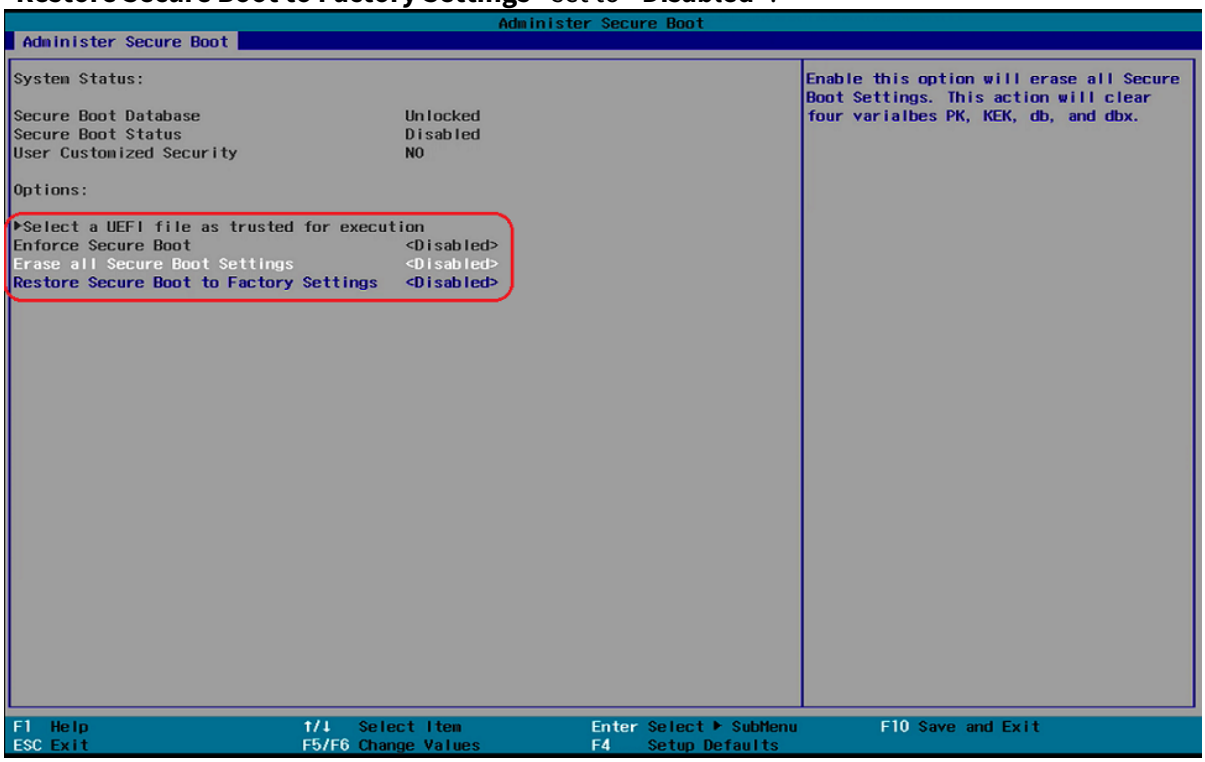
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Activating the Secure Boot Feature

1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the **Front Page** screen shown below.

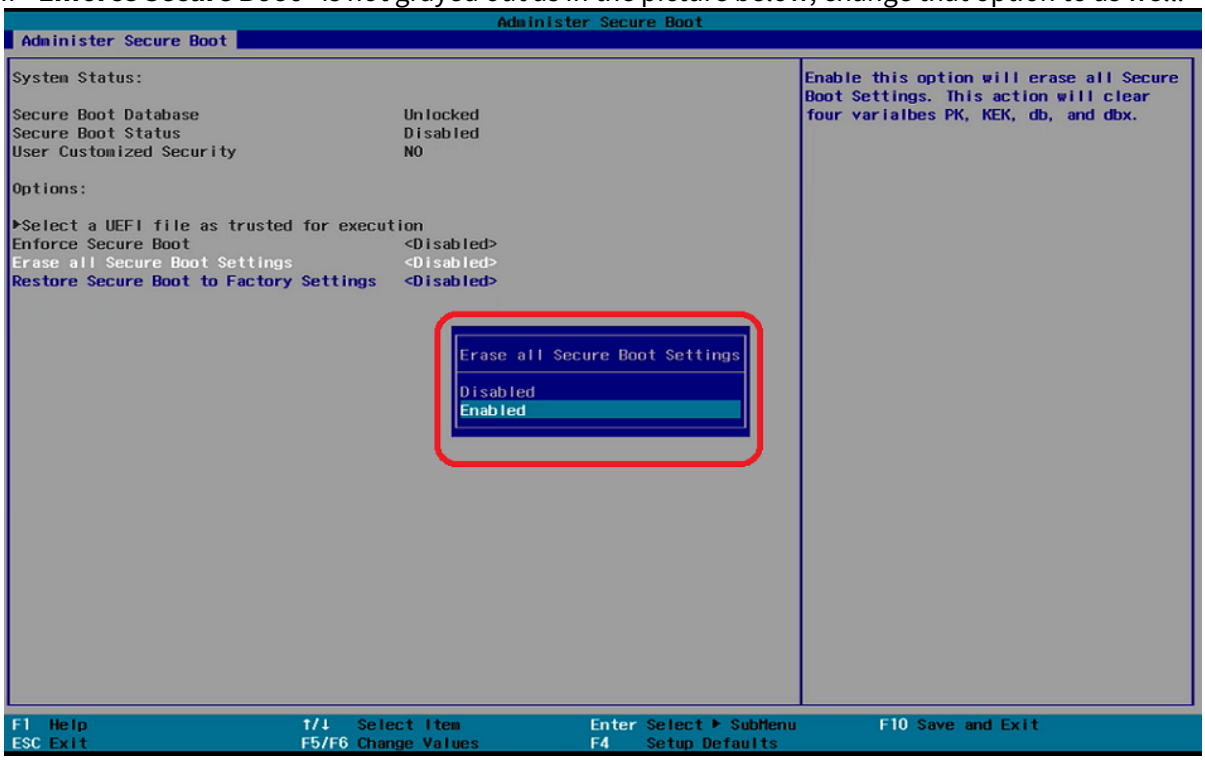


3. In the **Administer Secure Boot** screen, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.



4. Change both **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.

If **"Enforce Secure Boot"** is not grayed out as in the picture below, change that option to as well.



5. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes** with **[Yes]**.

The changes will be saved and the device will be rebooted.

6. As a last step, verify that Secure Boot is working, see Veryfing that UEFI Secure Boot is enabled.

Enabling UEFI Secure Boot in UD7-LX 20

UEFI Secure Boot is already a default setting in UD7-LX 20.

If you have disabled secure boot, you will need to reverse the settings you made.

Microsoft Windows 10 IoT

Enabling UEFI Secure Boot in UD3-W10 51

Prerequisites

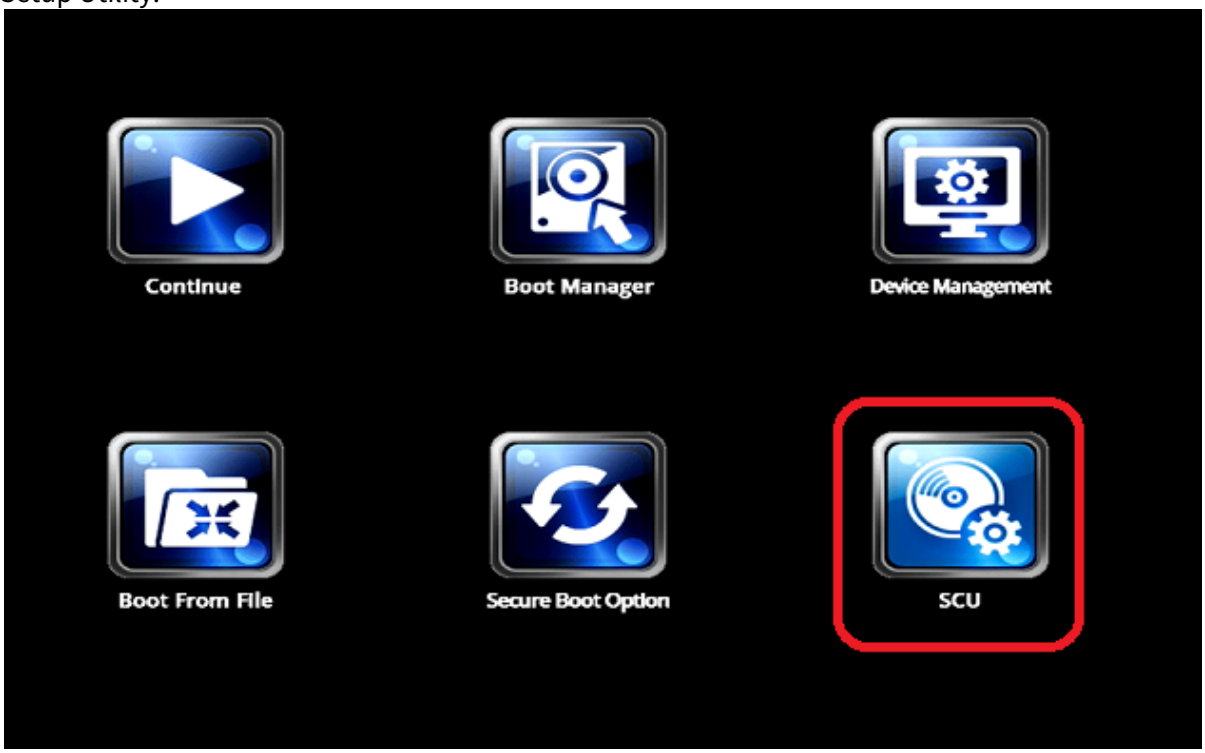
- Microsoft Windows IoT 4.03.100 or higher
- BIOS version 3.A. 13-11202017 or higher

> To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *3.A. 13-11202017* or newer.

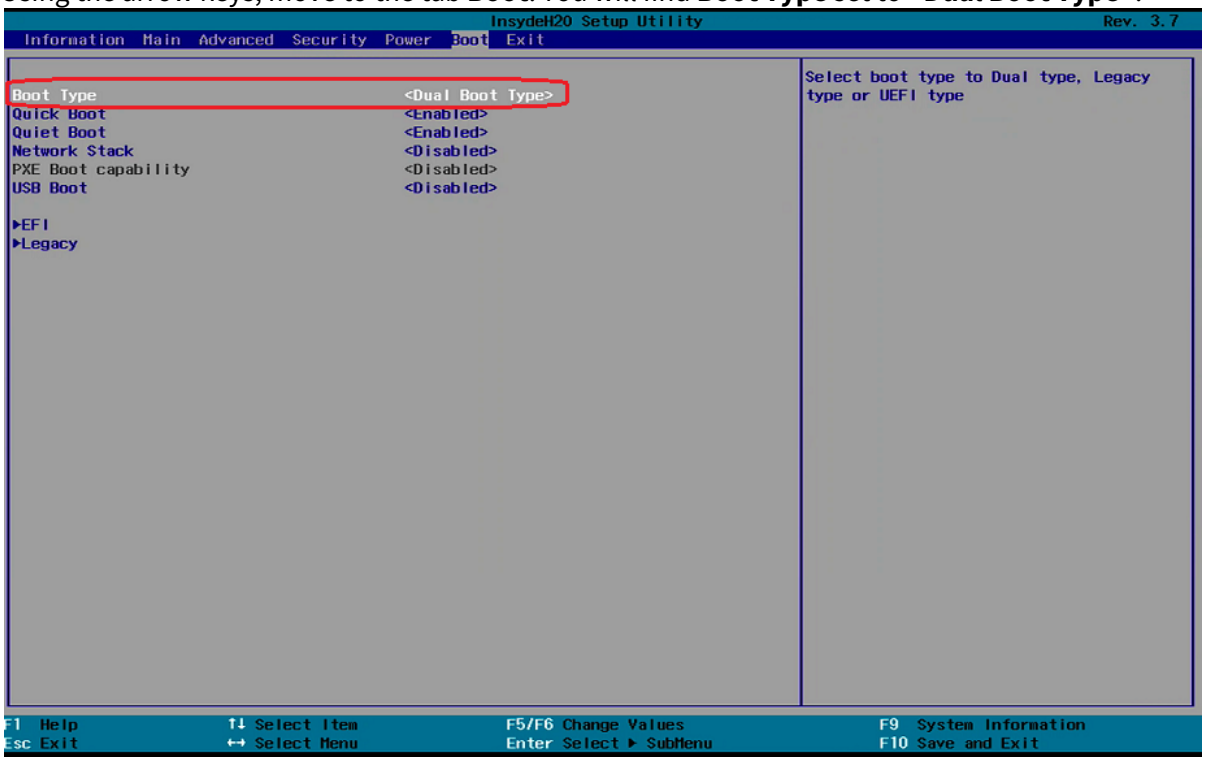
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Changing the Device's Boot Type to UEFI Boot

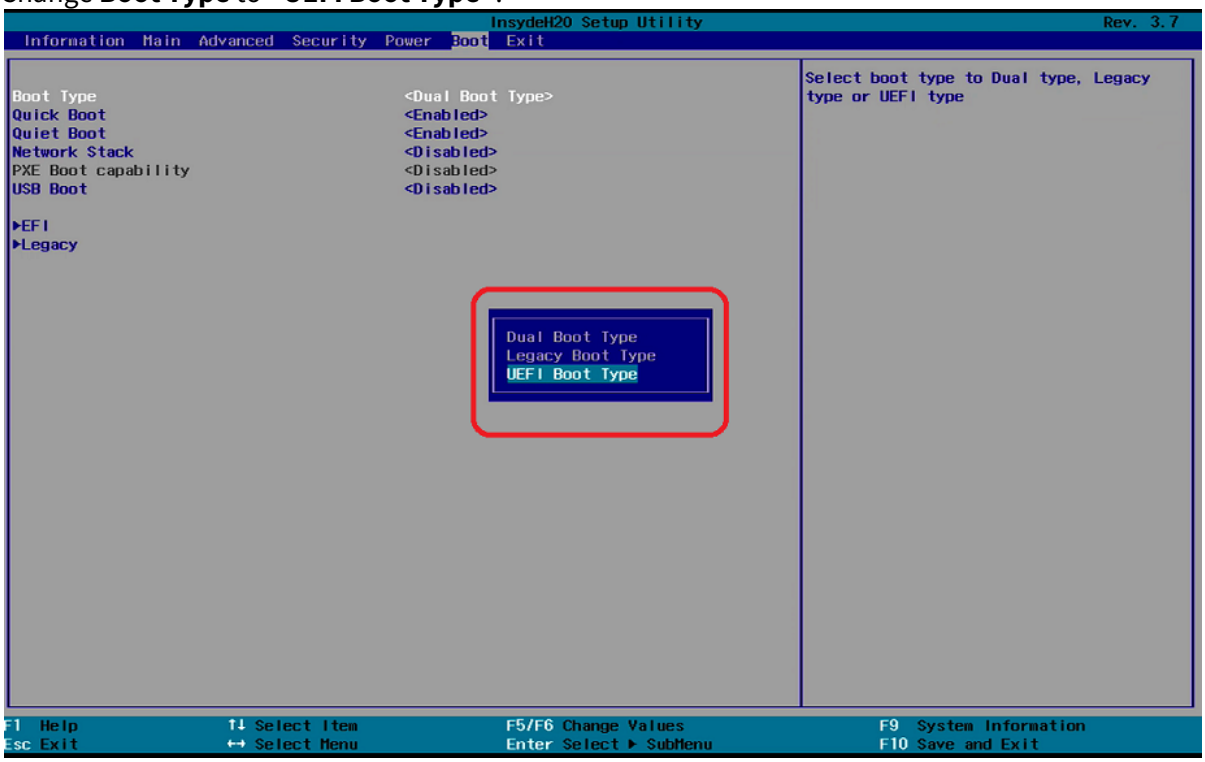
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



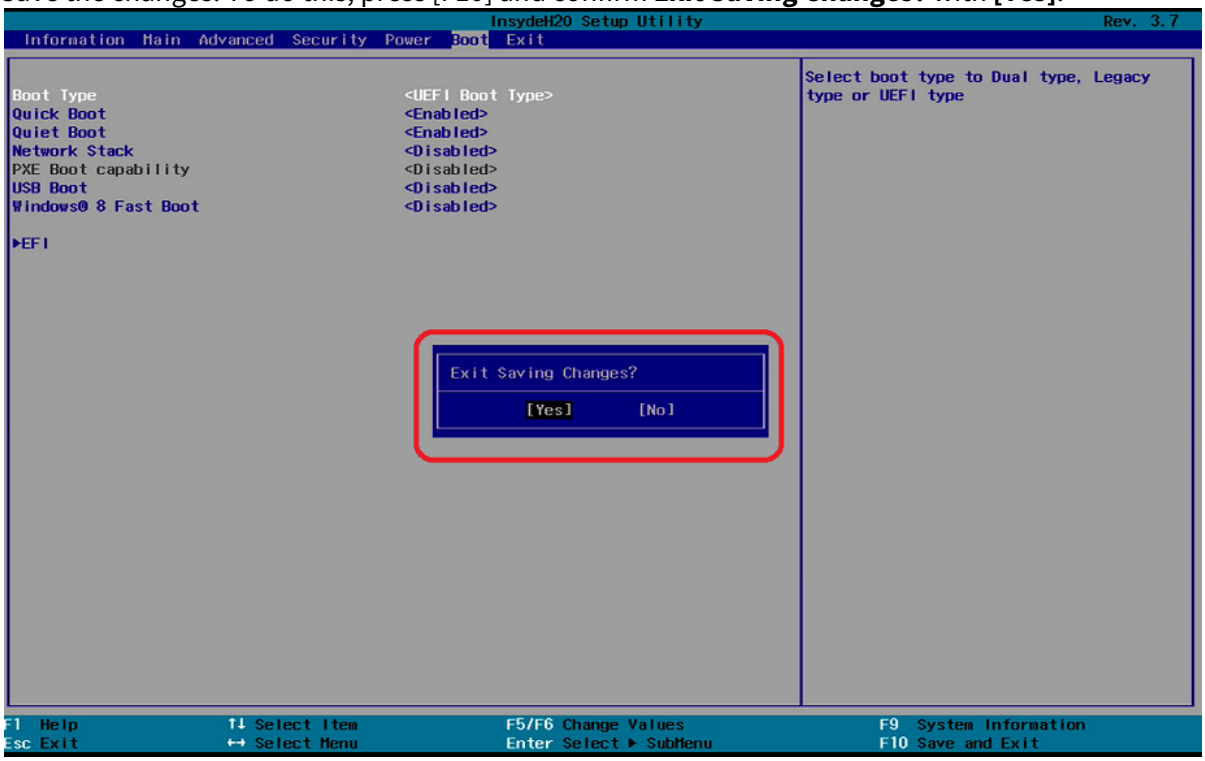
4. Using the arrow keys, move to the tab **Boot**. You will find **Boot Type** set to **<Dual Boot Type>**.



5. Change **Boot Type** to **<UEFI Boot Type>**.



6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.

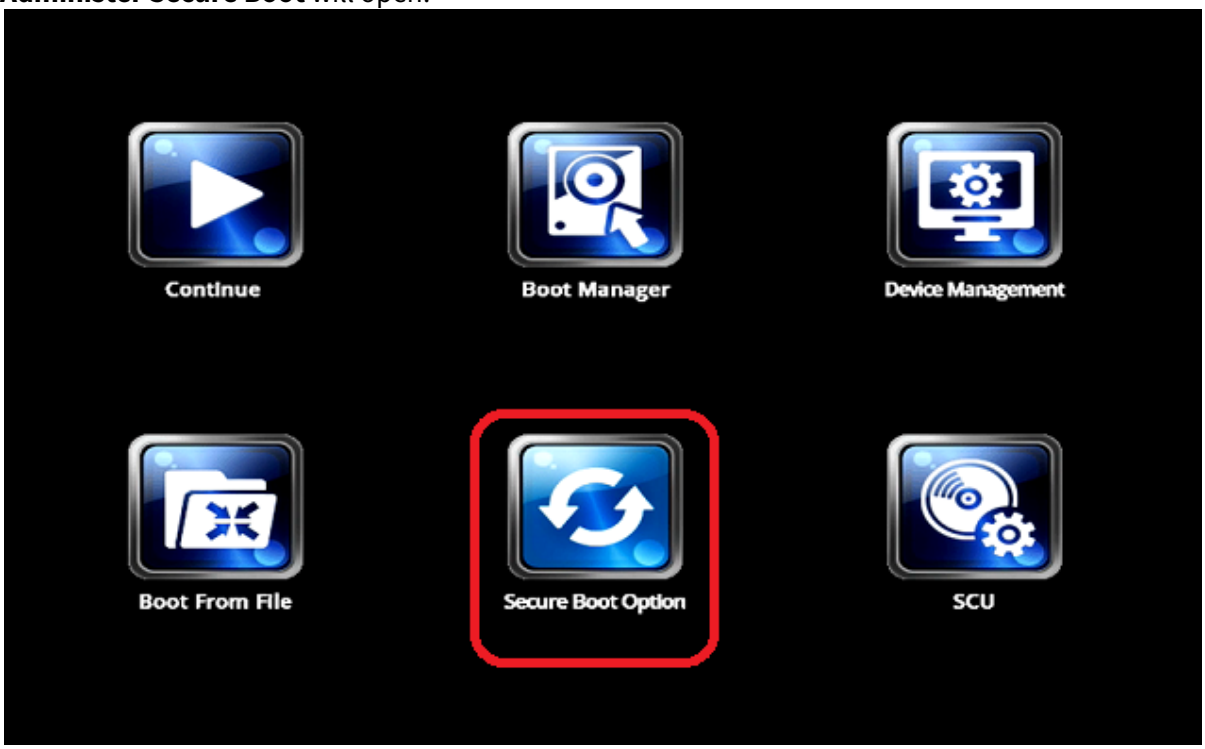


The changes will be saved and the device will be rebooted.

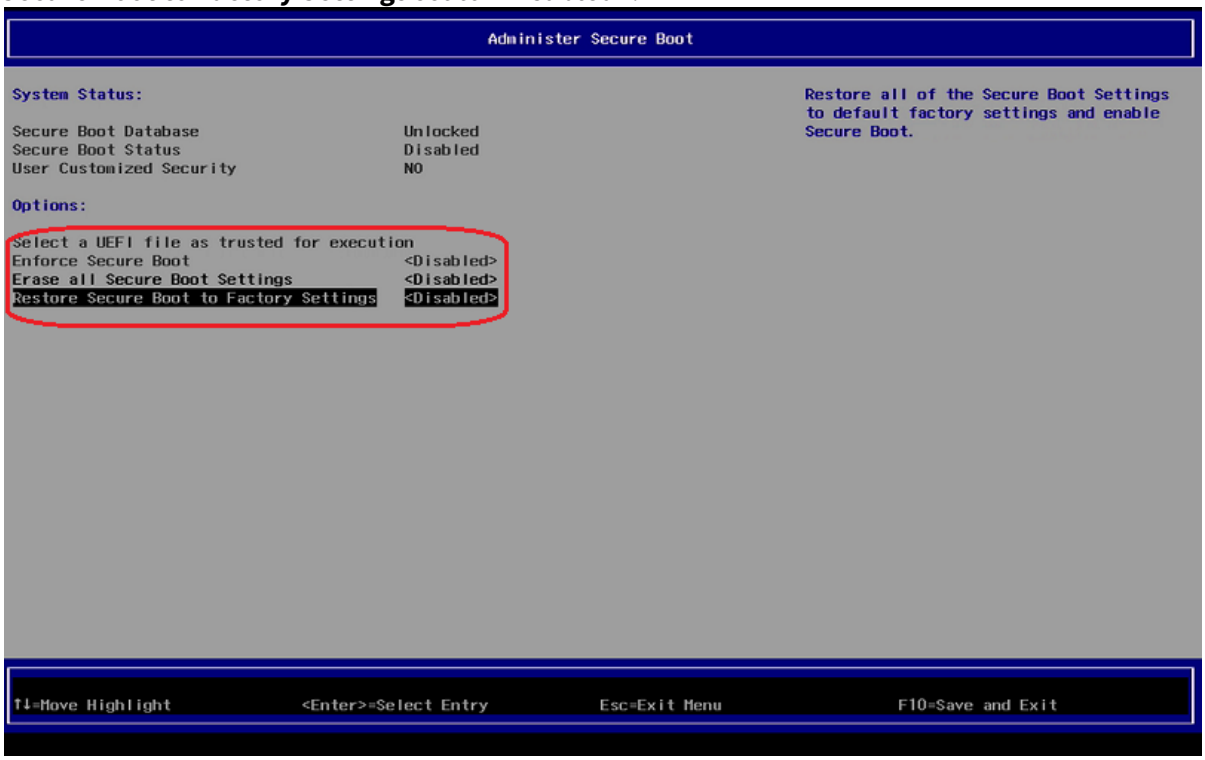
Activating the Secure Boot Feature

1. Turn on (or restart) the IGEL device.

2. Using the arrow keys, move to **Secure Boot Option** and press [ENTER]. The BIOS screen **Administer Secure Boot** will open.

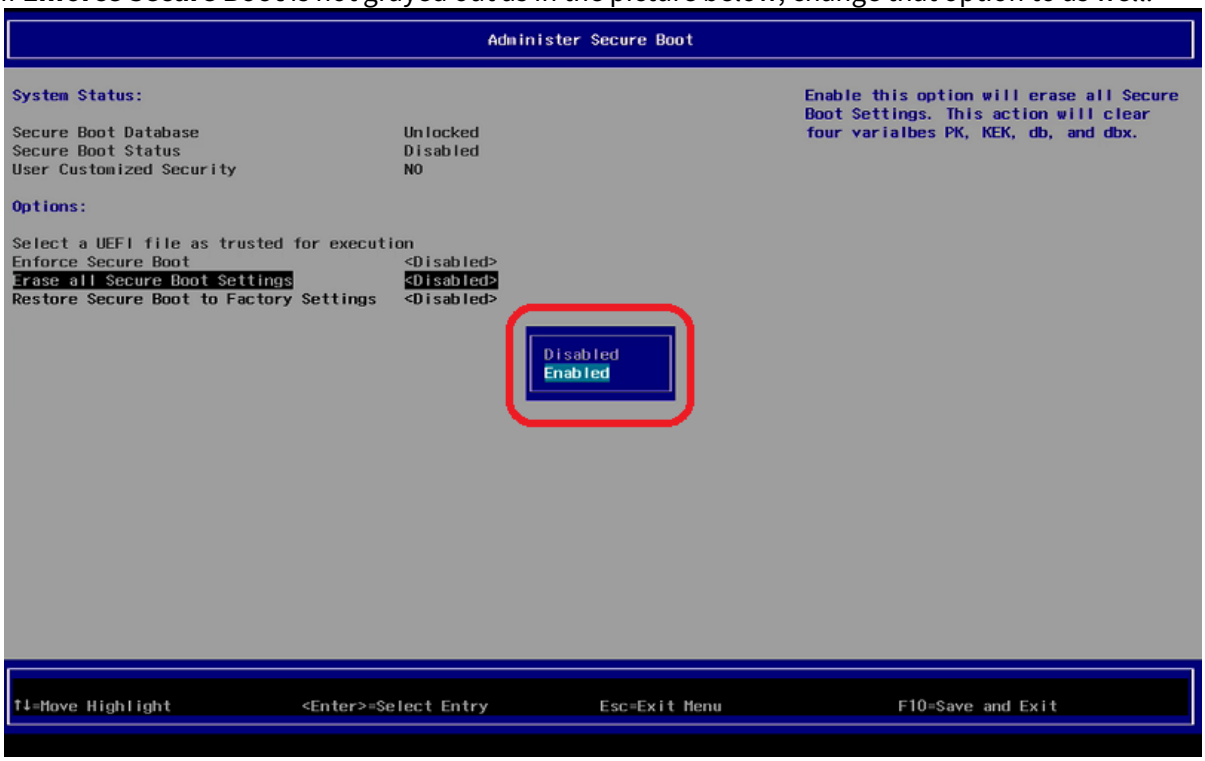


3. In the screen **Administer Secure Boot**, you will find **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** set to **<Disabled>**.

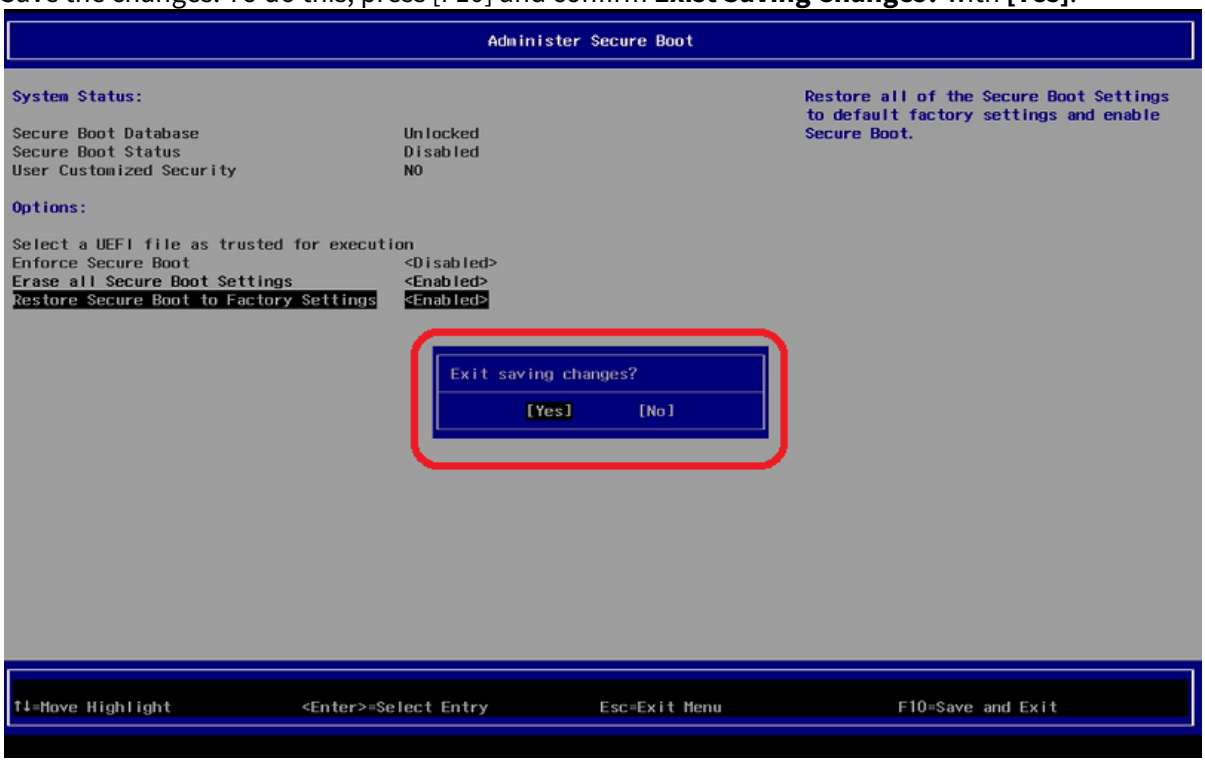


4. Change **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** to **<Enabled>**.

If **Enforce Secure Boot** is not grayed out as in the picture below, change that option to as well.



5. Save the changes. To do this, press [F10] and confirm **Exist Saving Changes?** with **[Yes]**.



The changes will be saved and the device will be rebooted.

6. As a last step, verify that Secure Boot is working, see Veryfing that UEFI Secure Boot is enabled.

Enabling UEFI Secure Boot in UD6-W10 51

Prerequisites

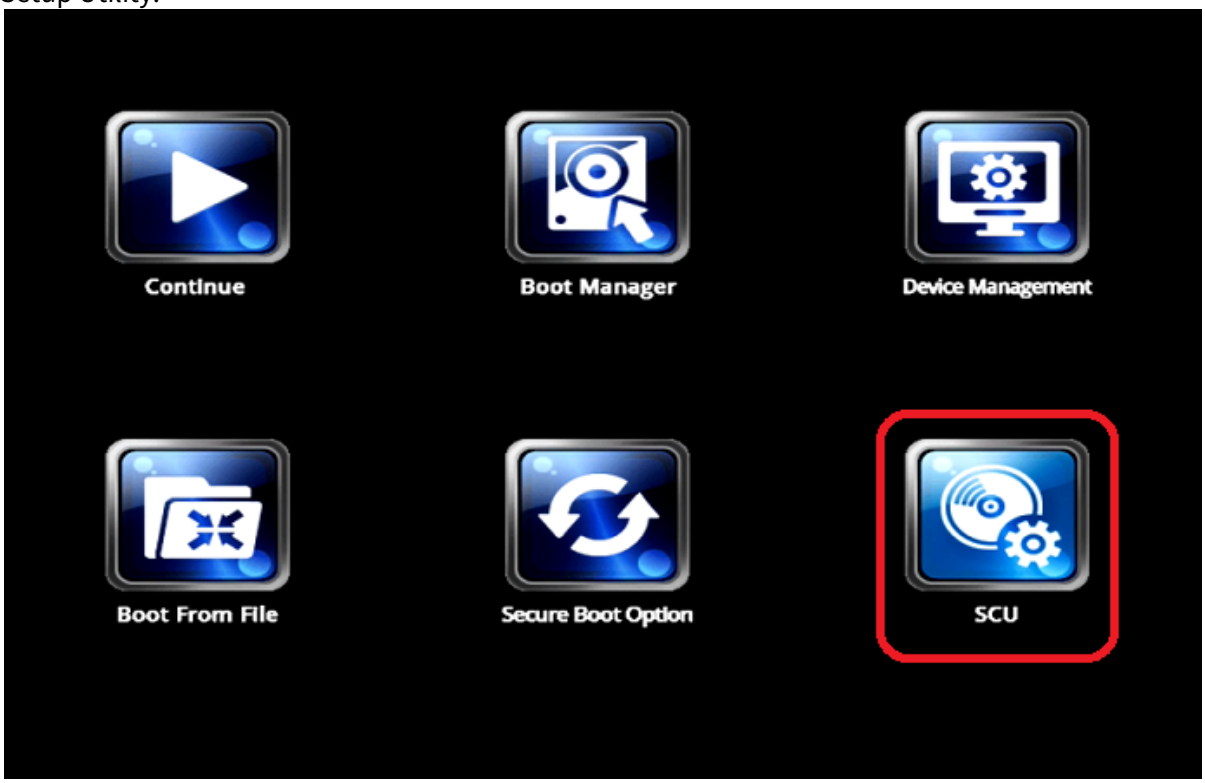
- Microsoft Windows 10 IoT 4.03.100 or higher
- BIOS version 3.9. 13-02202017 or higher

> To check the BIOS version, open the InsydeH20 Setup Utility as described below (step 3). Press [F9] to open the **System Information** window. In the **System Information** window, check that the BIOS version corresponds to *3.9. 13-02202017* or newer.

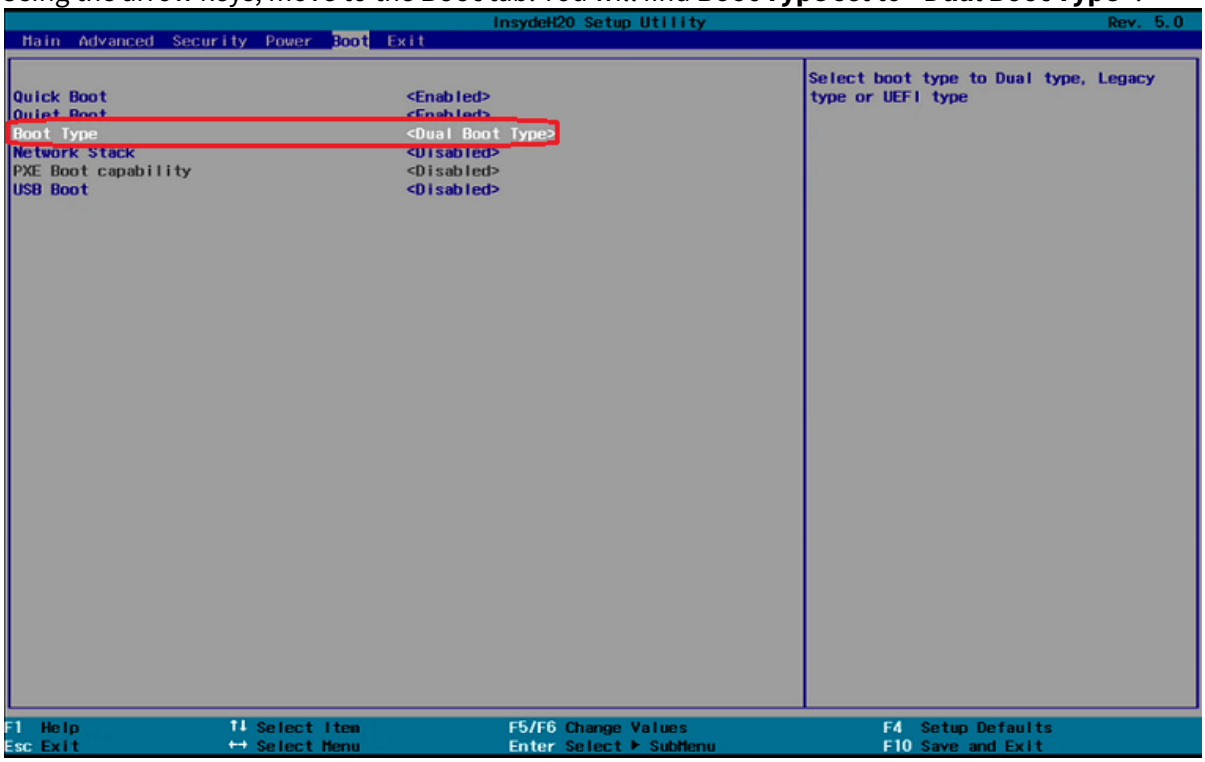
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Changing the Device's Boot Type to UEFI Boot

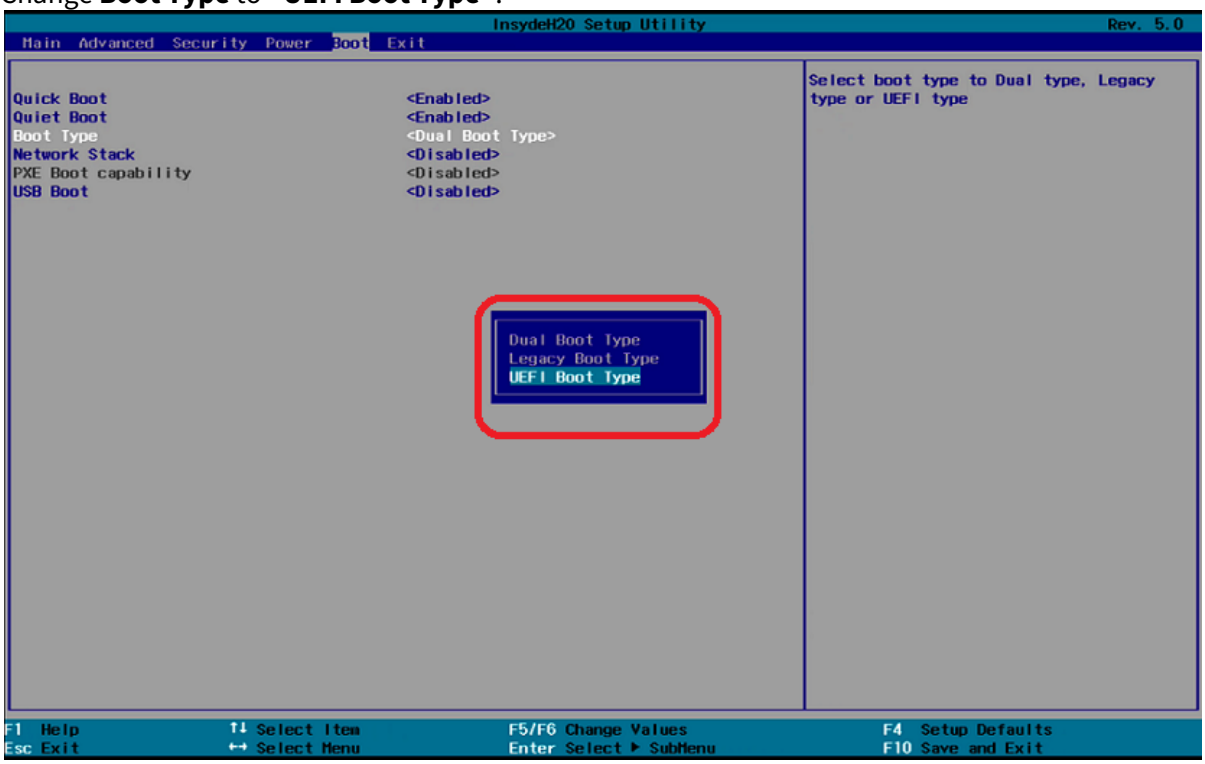
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



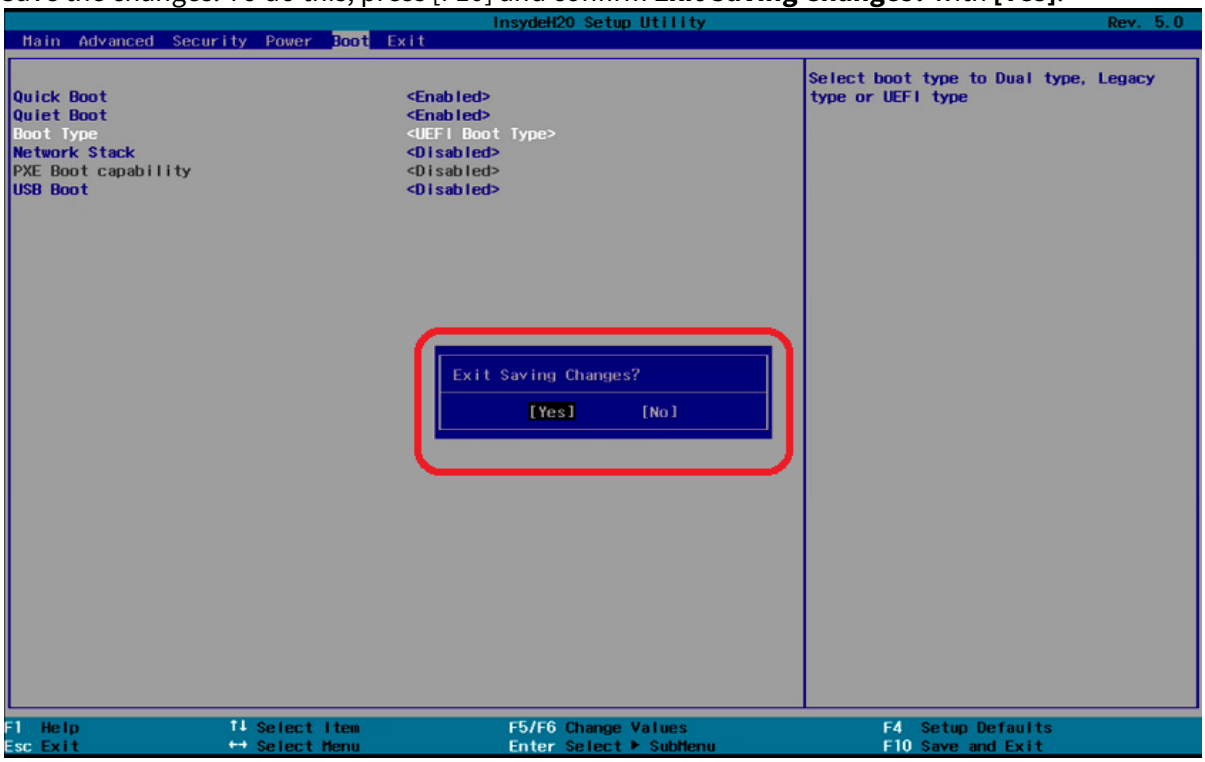
4. Using the arrow keys, move to the **Boot** tab. You will find **Boot Type** set to **<Dual Boot Type>**.



5. Change **Boot Type** to **<UEFI Boot Type>**.



6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.

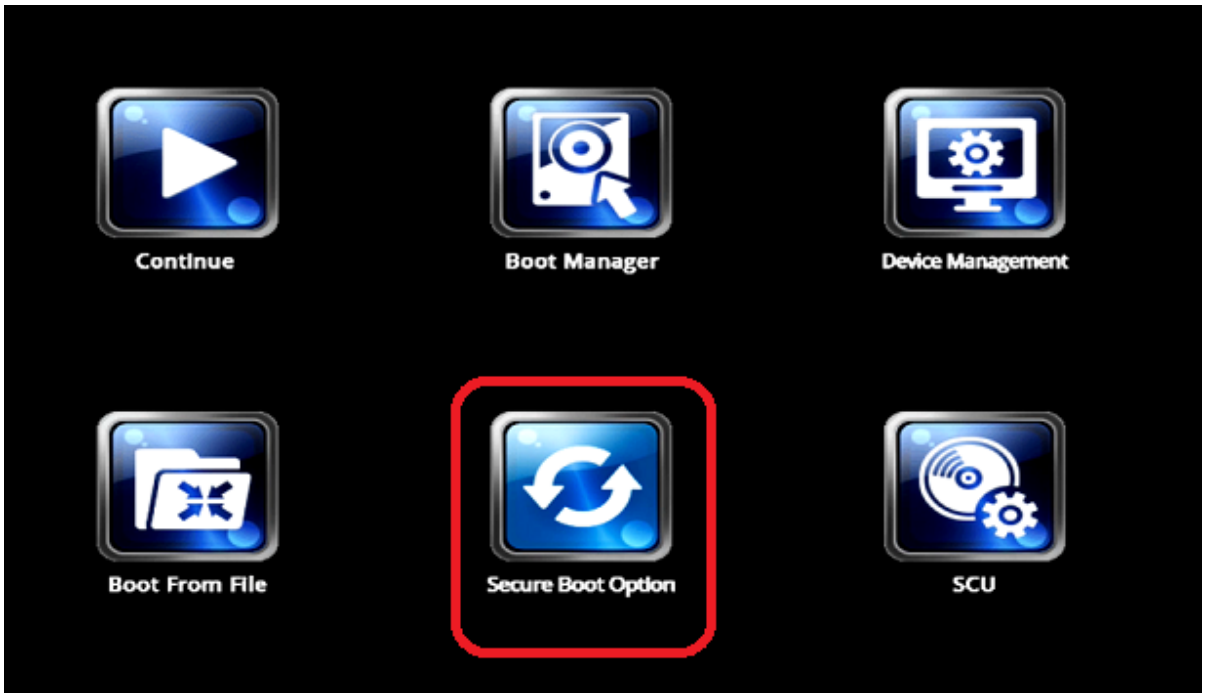


The changes will be saved and the device will be rebooted.

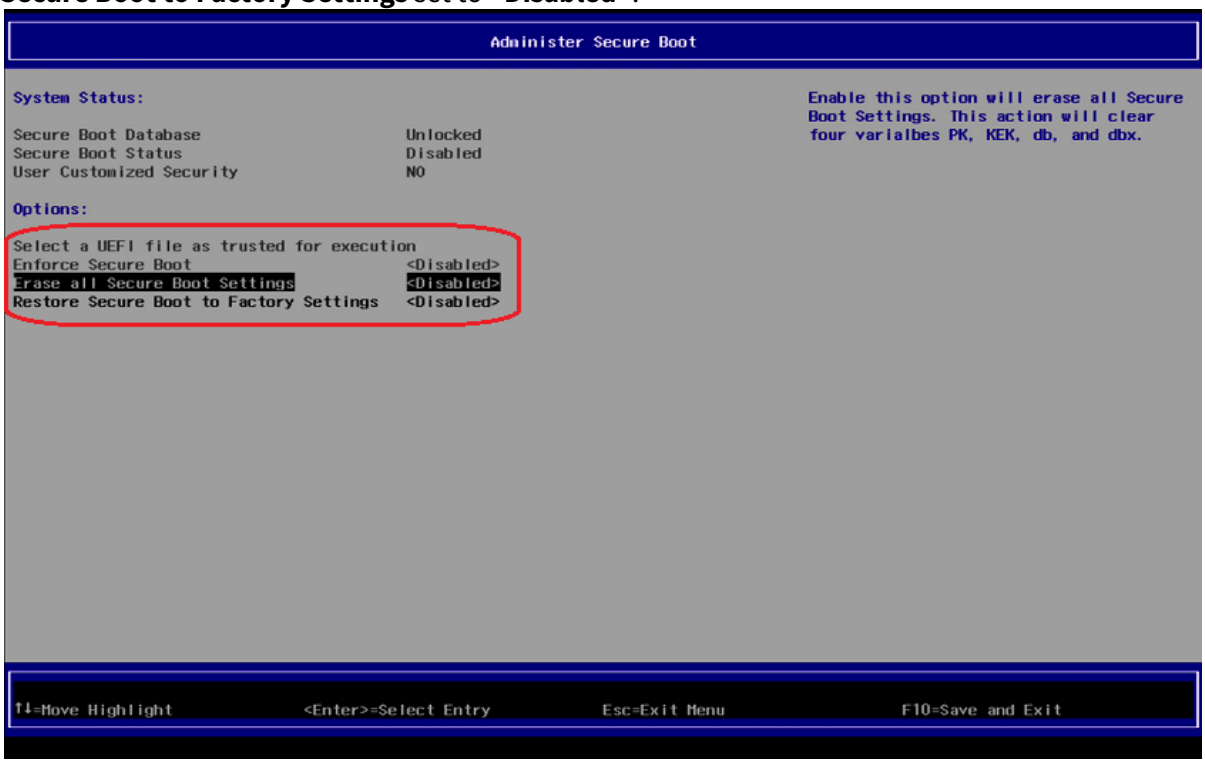
Activating the Secure Boot Feature

1. Turn on (or restart) the device.
2. During boot, hold the [DEL] key until you see the screen shown below.

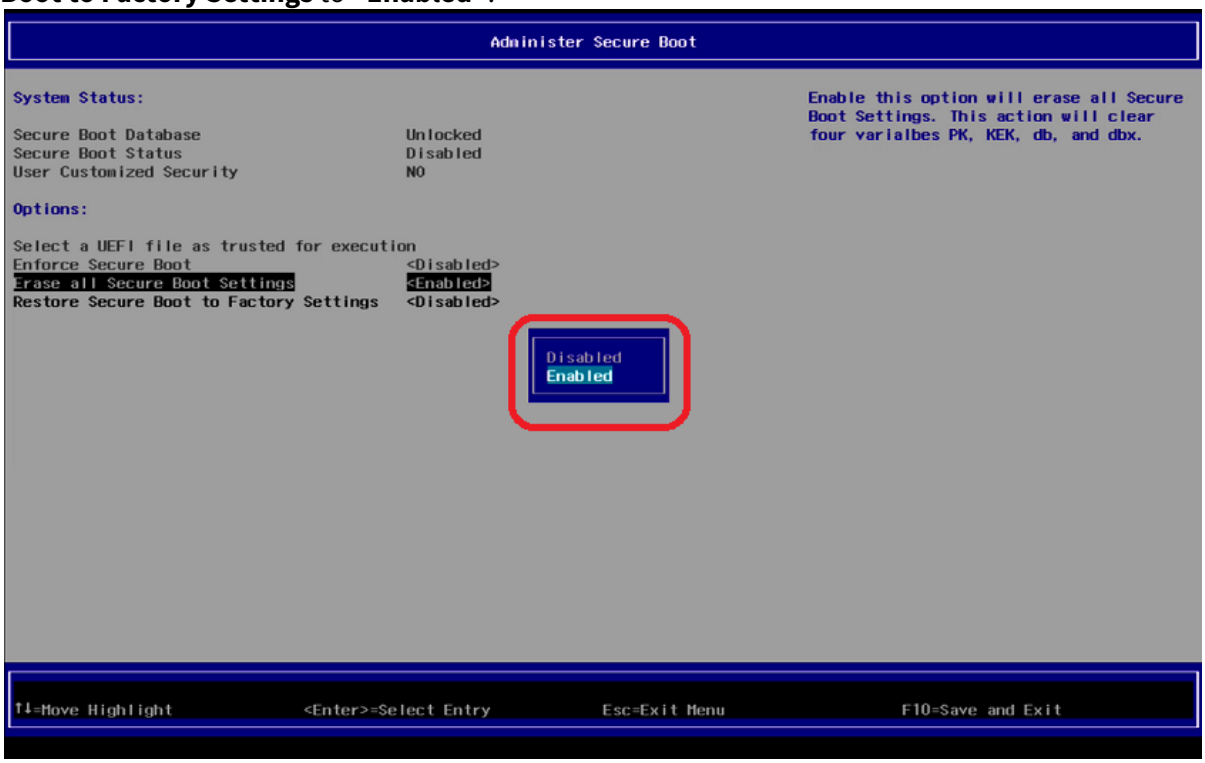
3. Using the arrow keys, move to the option **Secure Boot Option** and press [ENTER]. This will open the the screen **Administer Secure Boot**.



4. In the screen **Administer Secure Boot**, you will find **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** set to **<Disabled>**.

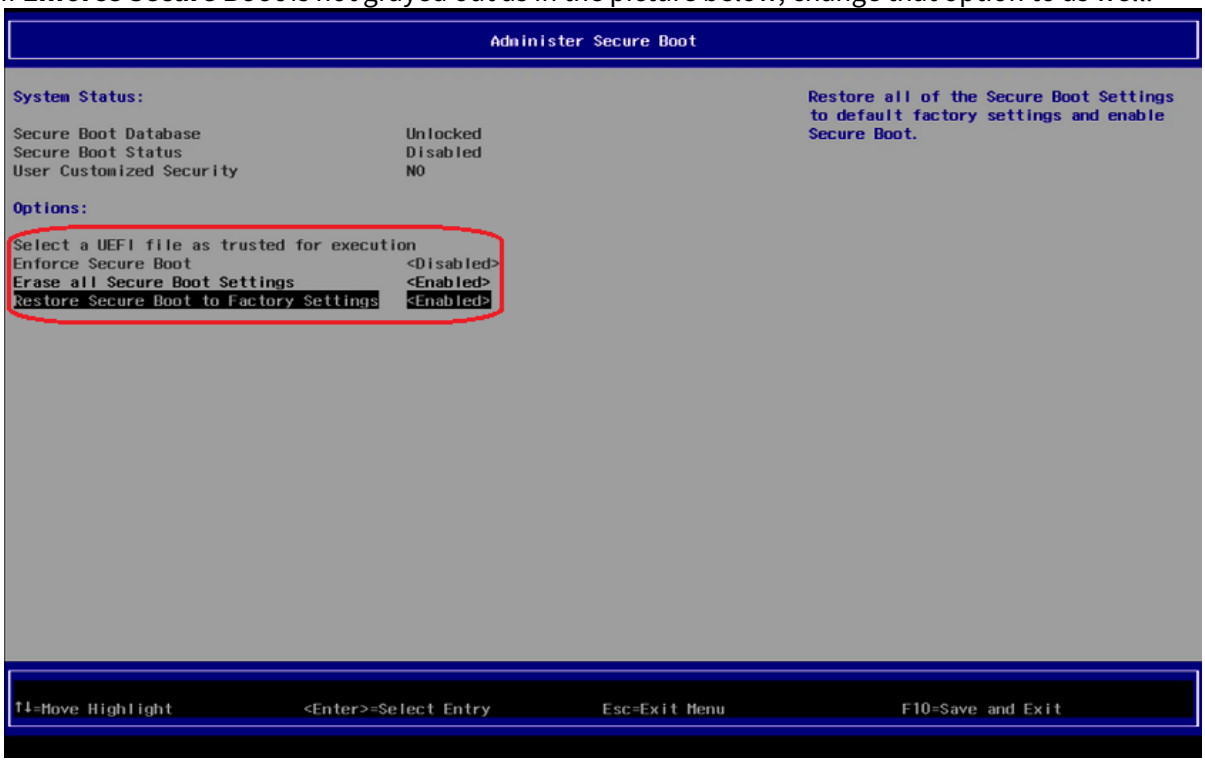


5. In the screen **Administer Secure Boot**, set **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** to **<Enabled>**.

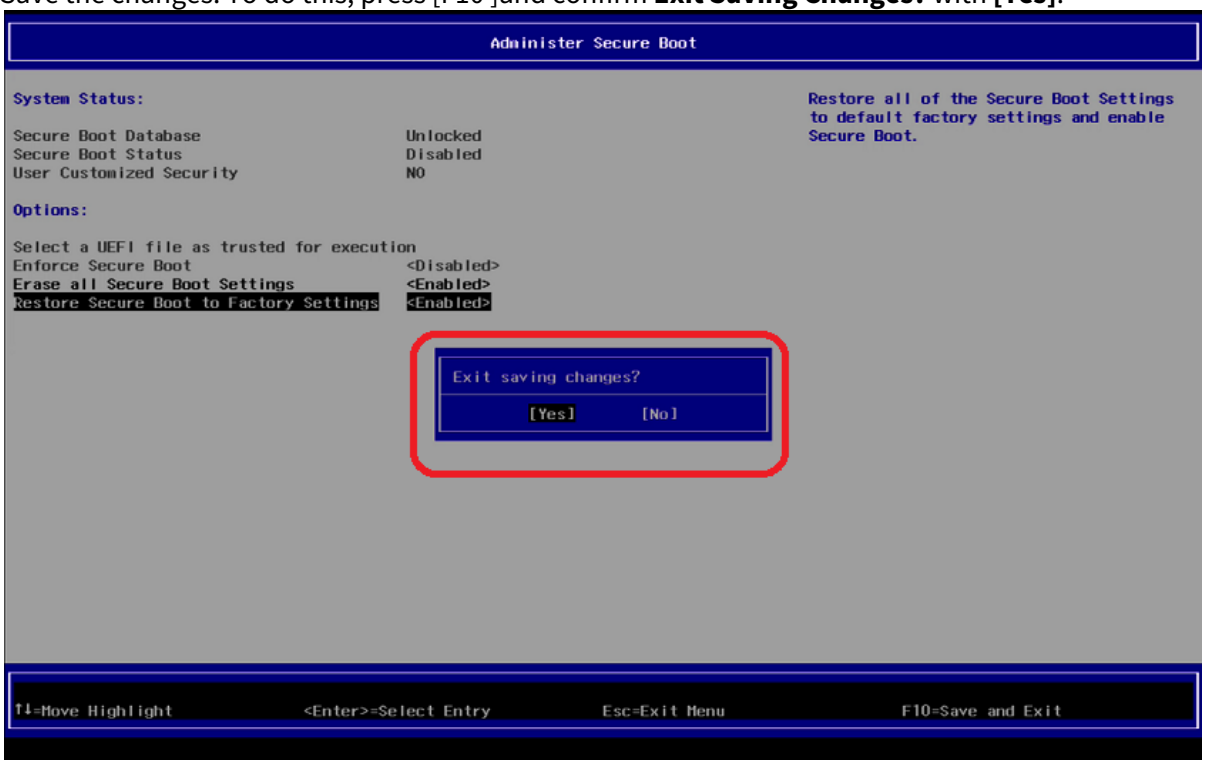


6. **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** are now set to **<Enabled>**.

If **Enforce Secure Boot** is not grayed out as in the picture below, change that option to as well.



7. Save the changes. To do this, press [F10]and confirm **Exit Saving Changes?** with **[Yes]**.



The changes will be saved and the device will be rebooted.

8. As a last step, verify that Secure Boot is working, see Veryfing that UEFI Secure Boot is enabled.

Enabling UEFI Secure Boot in UD7-W10 10

Prerequisites

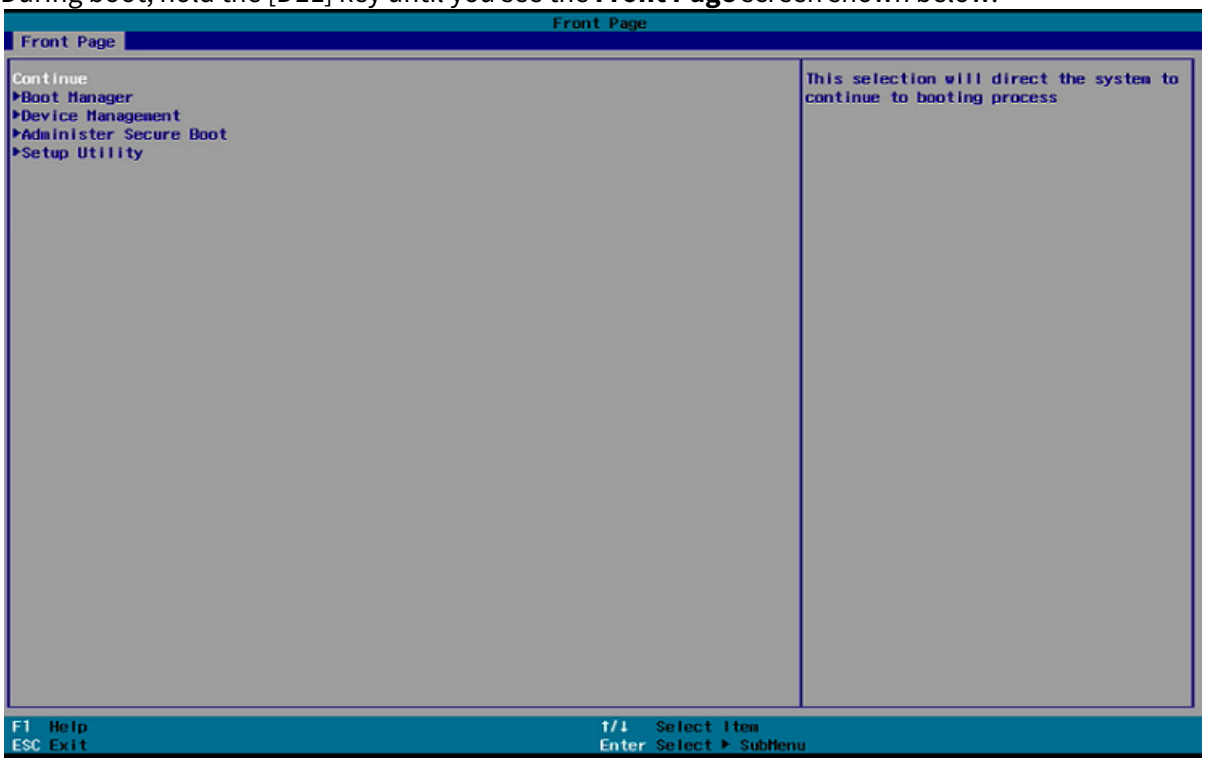
- Microsoft Windows IoT 4.03.100 or higher

UD7-W10 10 supports UEFI Secure Boot by default and no BIOS update is necessary.

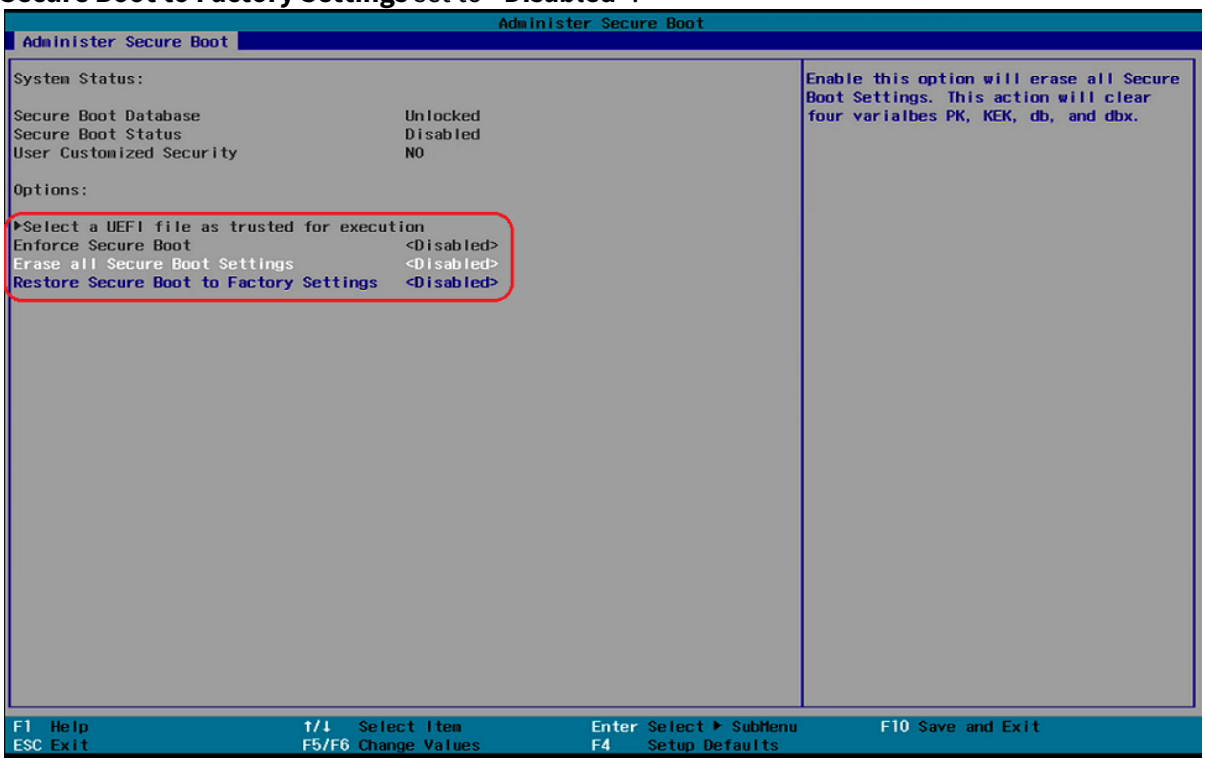
It is crucial to set a BIOS password to prevent users from disabling Secure Boot.

Activating the Secure Boot Feature

1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the **Front Page** screen shown below.

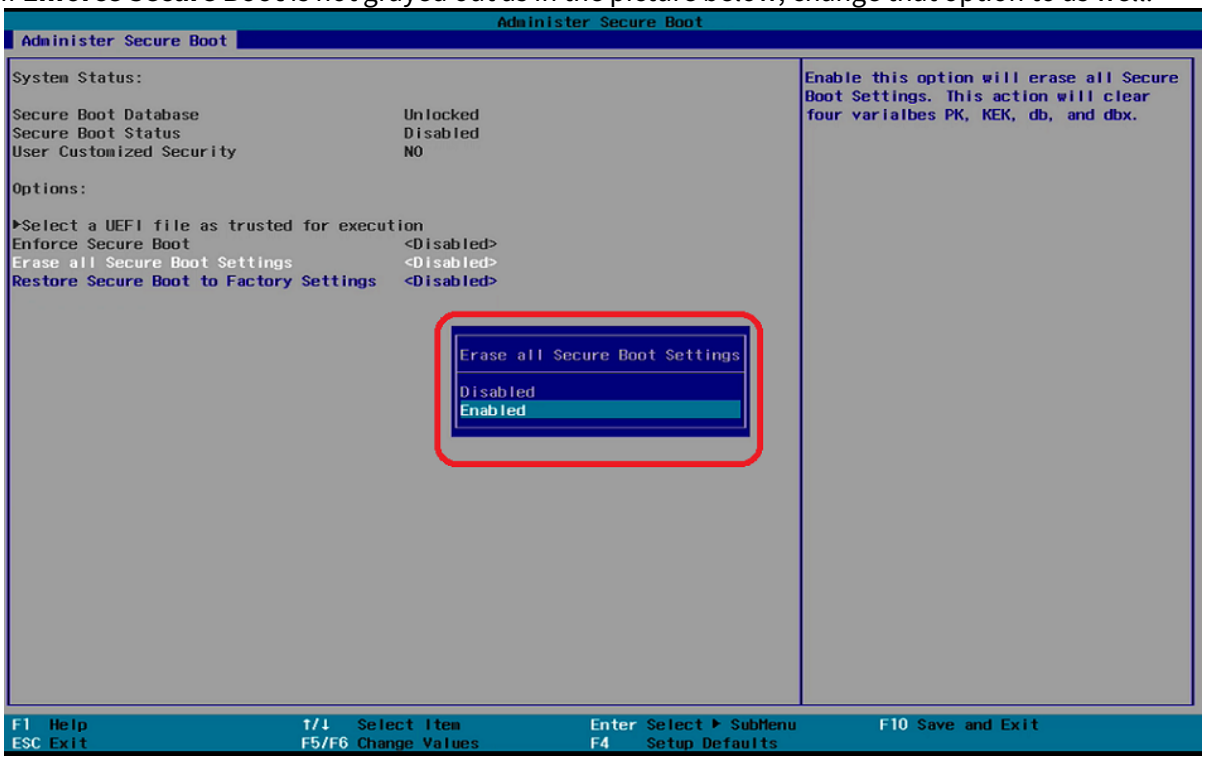


3. In the **Administer Secure Boot** screen, you will find **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** set to **<Disabled>**.



4. Change both **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** to **<Enabled>**.

If **Enforce Secure Boot** is not grayed out as in the picture below, change that option to as well.



5. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes** with **[Yes]**.

The changes will be saved and the device will be rebooted.

6. As a last step, verify that Secure Boot is working, see Veryfing that UEFI Secure Boot is enabled.

Verifying that Secure Boot is Enabled

It is important to verify that UEFI Secure Boot has been properly enabled.

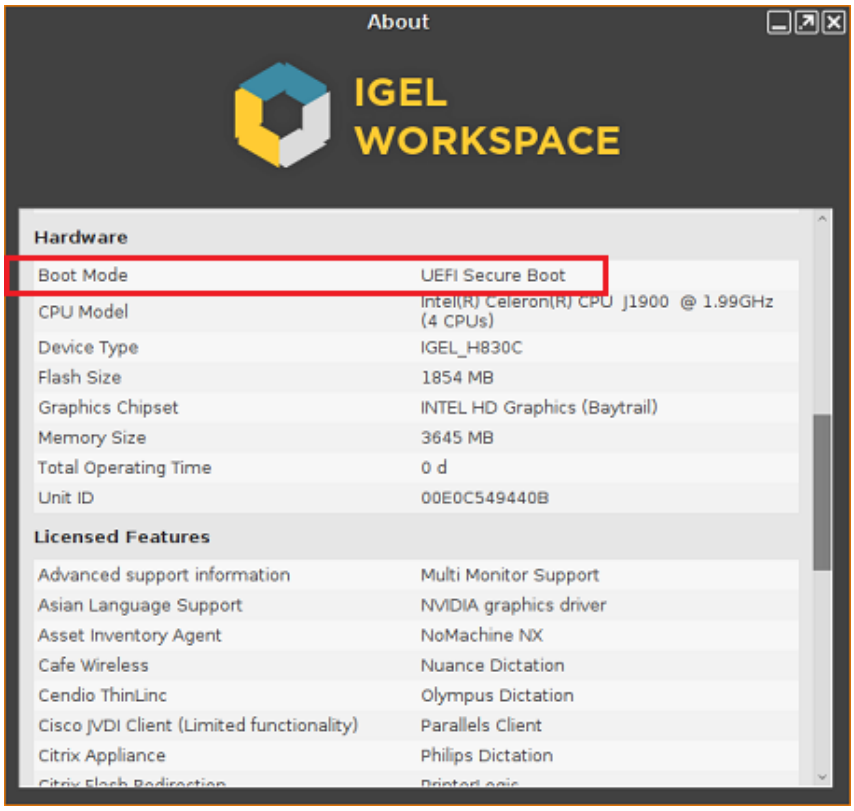
UEFI Secure Boot support is available in IGEL OS 10.04.100 or higher as well as Windows 10 IoT 4.03.100 or higher.

Check the following points to see whether UEFI Secure Boot has been properly enabled.

On IGEL OS 11.01.100 and Higher

- The boot splash contains a lock symbol.

- In the About window, **Boot Mode** is set to the value **UEFI Secure Boot**.



On IGEL OS 10.04.100 - 10.05.500

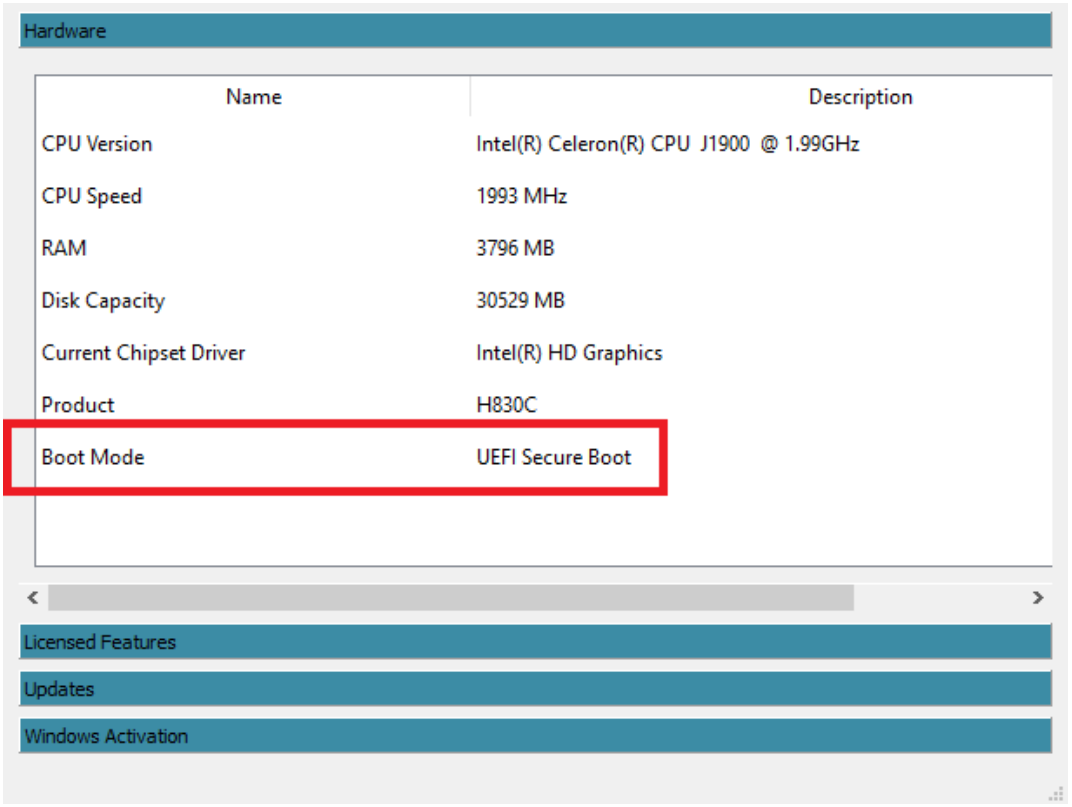
- The boot splash contains a lock symbol.

- In the About window, **Boot Mode** is set to the value **UEFI Secure Boot**.

On Microsoft Windows 10 IoT

- The boot splash contains a lock symbol.

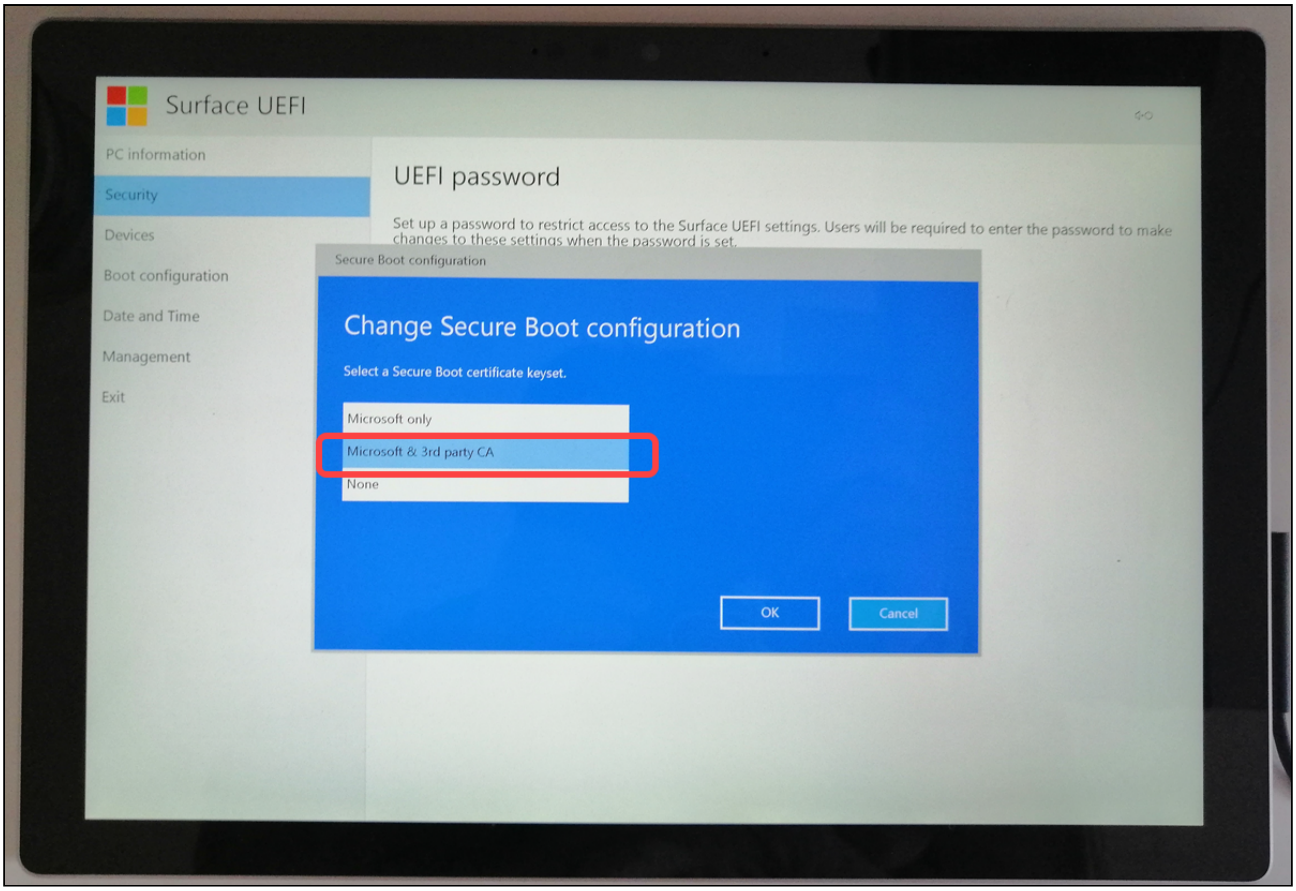
- In the IGEL Device Information tool, in the **Hardware** tab, **Boot Mode** is set to the value **UEFI Secure Boot**.

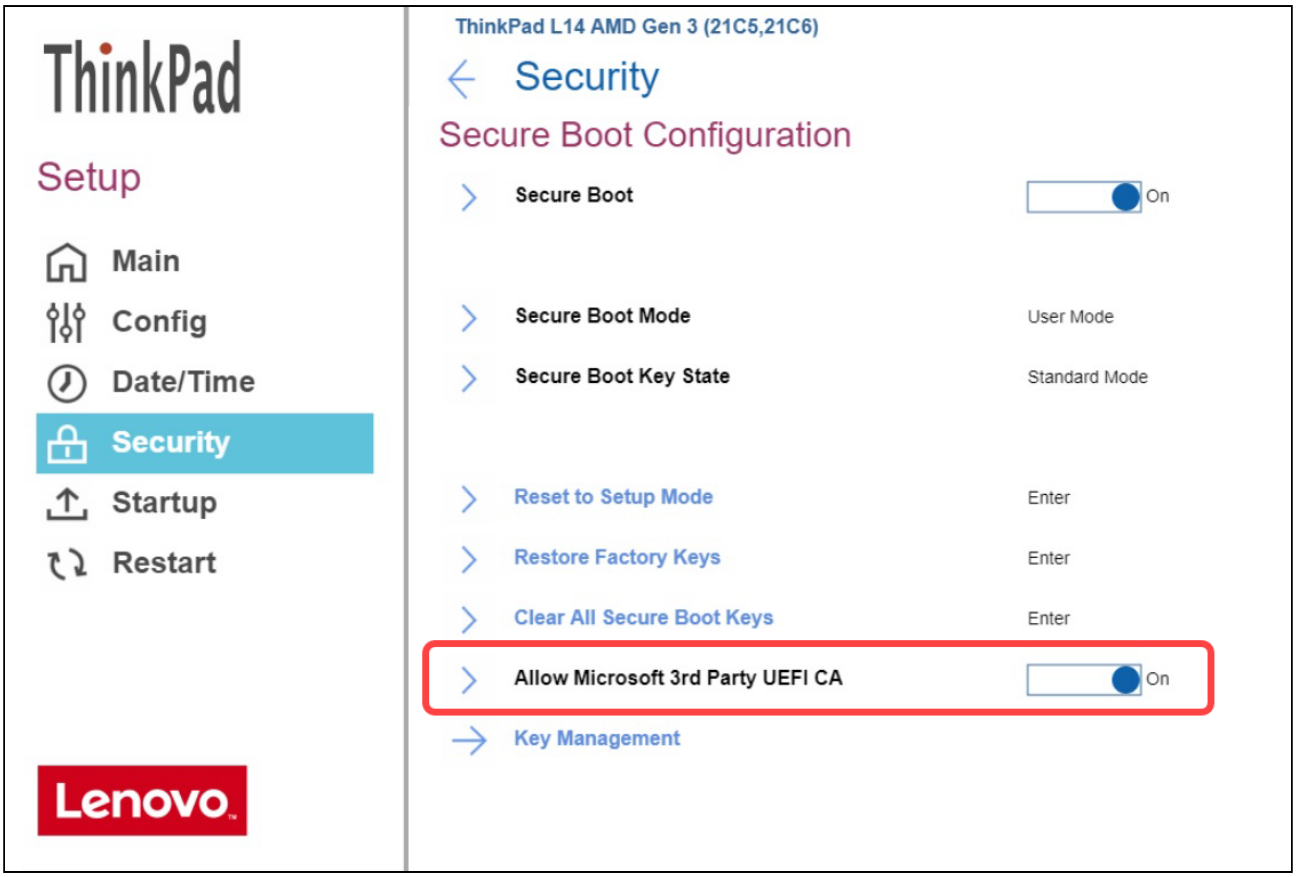

Hardware
Name
Description
CPU Version
Intel(R) Celeron(R) CPU J1900 @ 1.99GHz
CPU Speed
1993 MHz
RAM
3796 MB
Disk Capacity
30529 MB
Current Chipset Driver
Intel(R) HD Graphics
Product
H830C
Boot Mode
UEFI Secure Boot
Licensed Features
Updates
Windows Activation

Secured-Core PCs: Microsoft 3d-Party UEFI Certificate for Secure Boot

On secured-core PCs (see e.g. https://www.microsoft.com/en-us/windows/business/devices?col=secured-core-pcs), it is necessary to change the UEFI boot settings to **Microsoft 3rd-Party UEFI CA** in order to start the IGEL OS. This is required since by default, the UEFI only trusts Microsoft's 1st-party signing key for Windows, not the 3rd-party signing key that Microsoft uses to sign the IGEL OS.

Examples:




ThinkPad
Setup
Main
Config
Date/Time
Security
Startup
Restart
Lenovo
ThinkPad L14 AMD Gen 3 (21C5,21C6)
Security
Secure Boot Configuration
Secure Boot
On
Secure Boot Mode
User Mode
Secure Boot Key State
Standard Mode
Reset to Setup Mode
Enter
Restore Factory Keys
Enter
Clear All Secure Boot Keys
Enter
Allow Microsoft 3rd Party UEFI CA
On
Key Management

AMD Secure Processor

To enhance the security at the hardware level, IGEL implements the AMD Secure Processor technology. The AMD Secure Processor is a built-in dedicated security system that checks if the BIOS has a valid signature and thus secures the next step in the boot process. This ensures that only devices with a signed BIOS will boot.

For more information about the AMD Secure Processor, visit the AMD website https://www.amd.com/en/technologies/.

IGEL Devices with the Integrated AMD Secure Processor

- UD3 Model M350C
- UD7 Model H860C
- UD7 Model H850C(see page 137)

UD7 Model H850C

As from December 2019, IGEL UD7 model H850C is equipped with the AMD Secure Processor(see page 136).

> H850C devices manufactured before December 2019 do not include the AMD Secure Processor and cannot be upgraded.

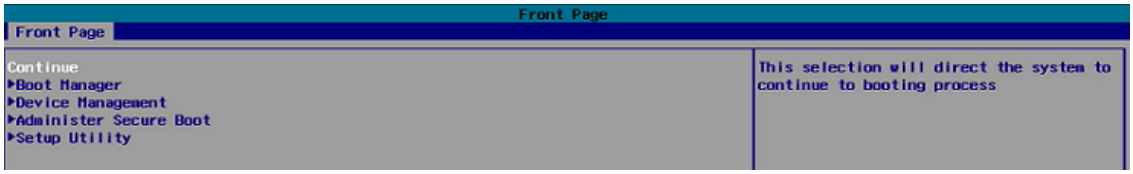
> The implementation of the AMD Secure Processor technology required mainboard and UEFI modification; backward compatibility is not supported.

> The AMD Secure Processor technology increases the system boot time between 3 and 4.5 seconds.

Features Distinguishing H850C Devices with the AMD Secure Processor

The following features distinguish H850C devices with the integrated AMD Secure Processor from H850C devices without it:

- BIOS version 3.9.13-10092019 and higher
  How to find out your BIOS version...
  a. Turn on (or restart) your UD7 device.
  b. During boot, hold the [DEL] key until you see the **Front Page** screen shown below.



  c. Choose **Setup Utility**.
  The **InsydeH20 Setup Utility** opens.
  d. Press [F9] to open the **System Information** window.
  e. In the **System Information** window, check **BIOS Version**.
- Hardware ID "LX-11", introduced with IGEL OS version 11.03.
- A black dot in the right bottom corner of the device label, which you can see if you pull out the black label holder located at the rear of the device:


www.igel.com
Thin Client 精簡型電腦
產品型號(Model Name): IGEL-H850C
輸入規格 (Input Rating): +12V⎓5A
製造商(Manufacturer): IGEL Technology GmbH
地址(Address):Hanna-Kunath-Str.31
28199 Bremen, Germany
Use only power supplies listed in the user manual.
CAN ICES-3(B)/NMB-3(B)
Made in China 中國製造 Designed in Germany 德國設計
LISTED
E308119
R3A044
RoHS

AMD Memory Guard

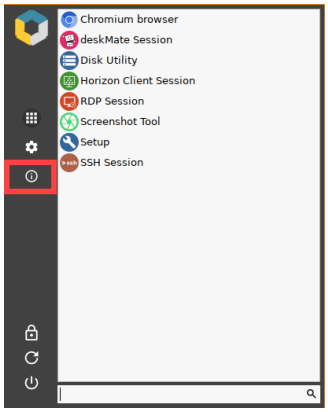
With AMD Memory Guard, IGEL enhances the security capabilities of the UD3 model M350C and UD7 model H860C.

AMD Memory Guard enables real-time memory encryption, which helps to protect against physical attacks and to secure data stored in RAM. The encryption is done on the basis of the randomly generated AES 128-bit encryption key and performed as such by the AMD Secure Processor(see page 136) integrated in the IGEL device.

For more information about AMD Memory Guard, see https://www.amd.com/system/files/documents/amd-memory-guard-white-paper.pdf.

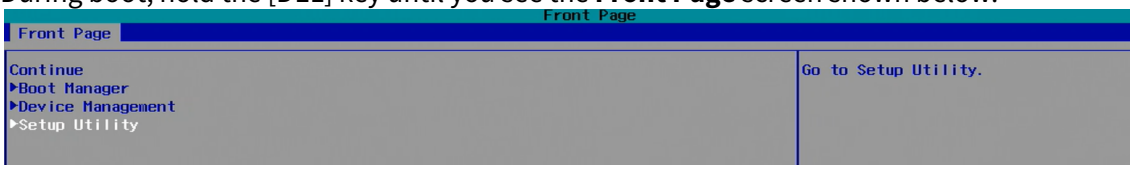
Activation / Deactivation

- AMD Memory Guard is available and activated by default as of BIOS version 3.5.13A-07222020.
- The activation/deactivation status is indicated in the **About** window, accessible via the icon , as of IGEL OS 11.04.100.



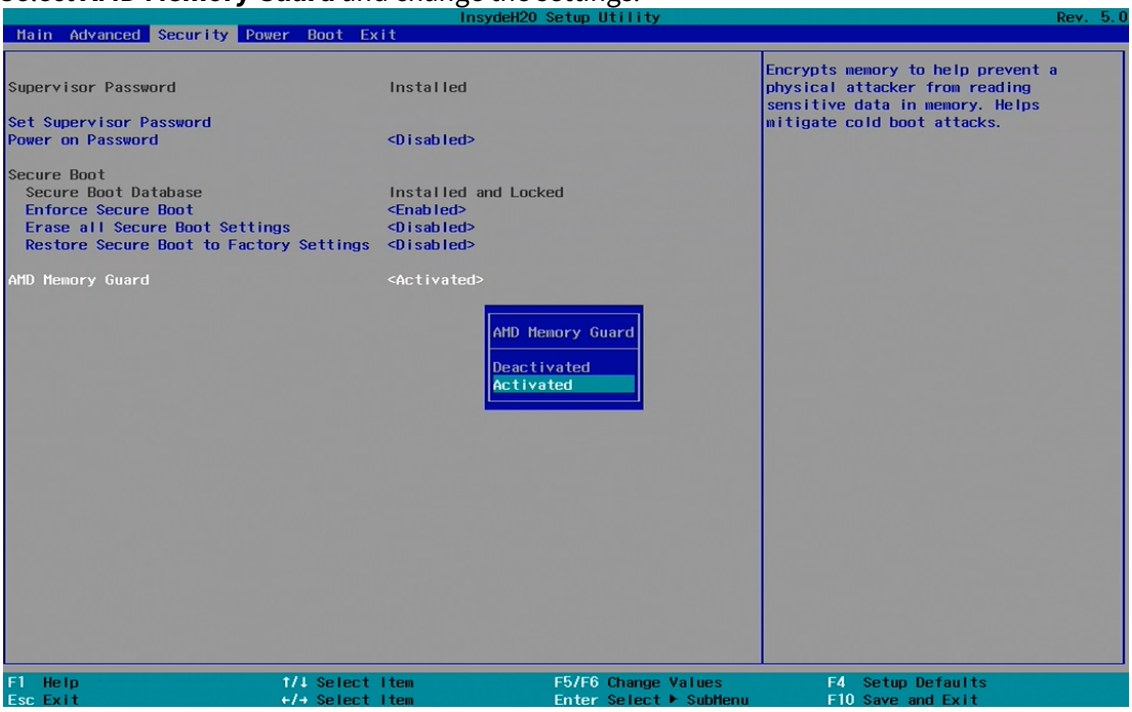
- AMD Memory Guard can be deactivated in BIOS under **Setup Utility > Security**.
  How to deactivate AMD Memory Guard

  a. Turn on (or restart) your device.
  b. During boot, hold the [DEL] key until you see the **Front Page** screen shown below.



  c. Choose **Setup Utility**.
  The **InsydeH20 Setup Utility** opens.
  d. Go to **Security**.

e. Select **AMD Memory Guard** and change the settings.



f. Press [F10] to save the changes.

As AMD Memory Guard has only a minor impact on system performance – e.g. on M350C, the reduction equals to 1-1.5% – it is advisable to leave the feature activated.

Security FAQs

Which OpenSSL Version and Ciphers Does IGEL Linux 4.10 Ship With?

Environment: IGEL Linux 4.10

IGEL Linux 4.10 uses the OpenSSL package 1.0.2g-1ubuntu4.10.

To see the list of ciphers, open a local terminal and issue the following command: `openssl ciphers`

> You do not have to be root to run this command.

BSI Grundschutz

This document is available in German only.

Anleitung zum IT-Grundschutz-konformen Betrieb von IGEL OS 11.03.100

This document is available in German only.

Über dieses Dokument

This document is available in German only.

Grundsätzliche Vorgaben zur Administration

This document is available in German only.

Fernwartung

This document is available in German only.

Zugriffskontrolle

This document is available in German only.

Absicherung des Bootvorgangs

This document is available in German only.

Schutz bei Diebstahl oder Defekt

This document is available in German only.

Schutz vor Manipulation

This document is available in German only.

Einschränken der Benutzerumgebung

This document is available in German only.

Logging and Log Evaluation

Prerequisites

Teleworking computers should have a logging function and should have a log evaluation function.

Note

IGEL recommends leaving logging enabled by default (authentication, kernel, and daemons) and limiting the desired parameters by filtering during evaluation.

Action: Forward Logs to Log Analyzer

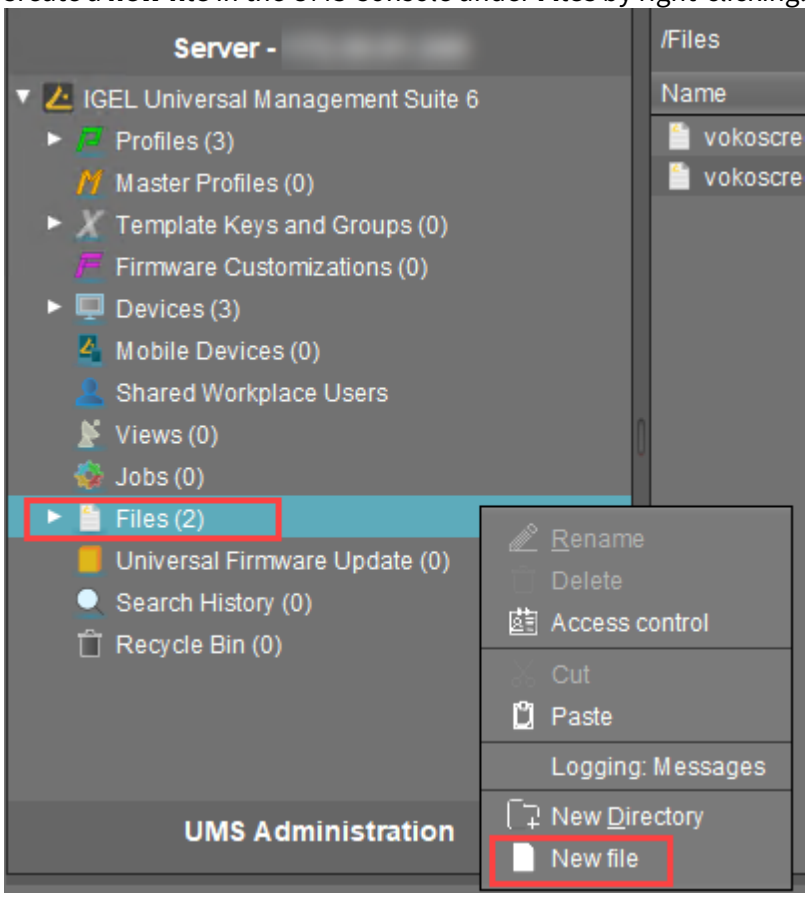
Use a log collector and analyzer, which allows the archiving and analysis of logs according to many aspects, such as Graylog, Splunk or the Elastic-Logstash-Kibana-Stack (ELK). Their evaluation function must be able to differentiate according to the types of data required for logging (for example, filtering all unauthorized access to all resources in a given period of time). The evaluation function must generate evaluable (readable) reports so that no security-critical activities are overlooked.

Such solutions can receive log data via rsyslog interface with TLS encryption. In IGEL OS, configure the forwarding as follows:

Installing the Certificate

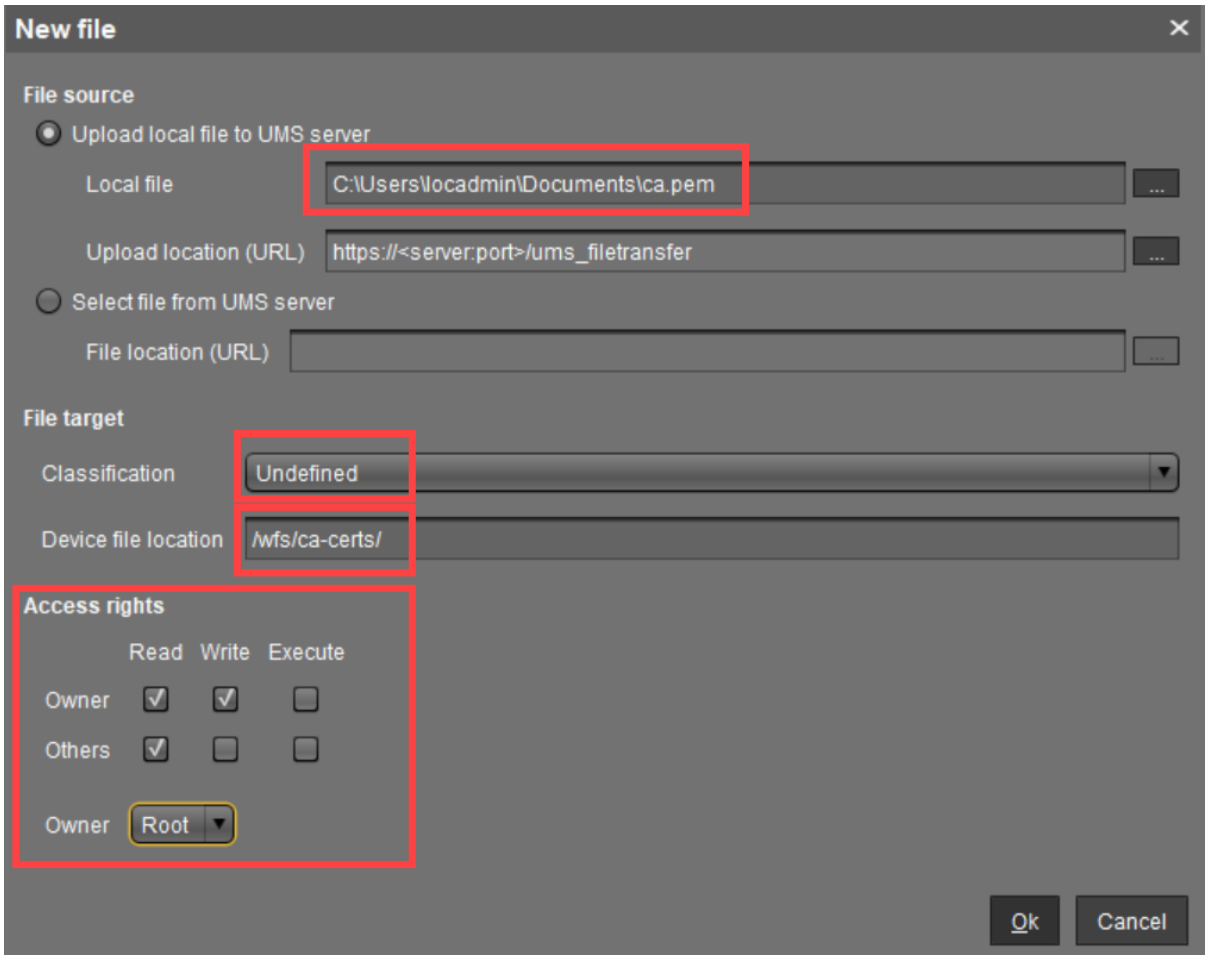
If the X.509 certificate of your log collector is not signed by a CA known to IGEL OS, install the CA root certificate of the signer as follows:

1. Create a **new file** in the UMS Console under **Files** by right-clicking.



2. Under **Local file**, select the CA root certificate file `ca.pem` in PEM format and upload it.
3. Under **Classification**, select "Undefined".
4. Enter `/wfs/ca-certs/` for the **Device file location**.

5. Enable read and write permission for the **Owner**, read permission for **Others** and set the **Owner** to **Root**.

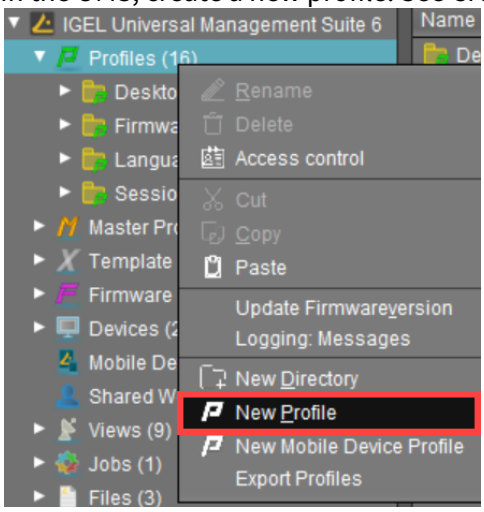


6. Click **Ok**.
7. Assign the file object to the desired devices.

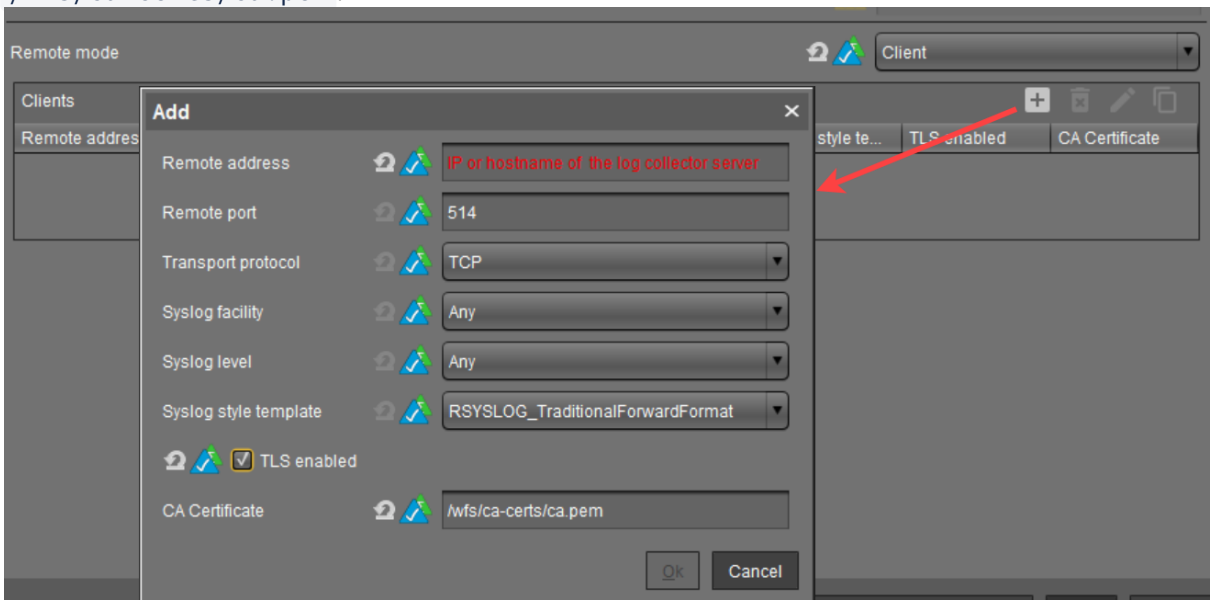
Configuration of Log Forwarding on IGEL OS

As of IGEL OS 11.06.100, you can configure the log forwarding with TLS encryption as follows:

1. In the UMS, create a new profile. See Creating Profiles.



2. In the configuration dialog, go to **System > Logging**.
3. Set **Remote mode** to "Client".
4. Click the **Add** button.
5. Make the required settings and activate **TLS enabled**.
6. Under **CA certificate**, specify the path to the CA root certificate you have installed previously, e.g. `/wfs/ca-certs/ca.pem`.

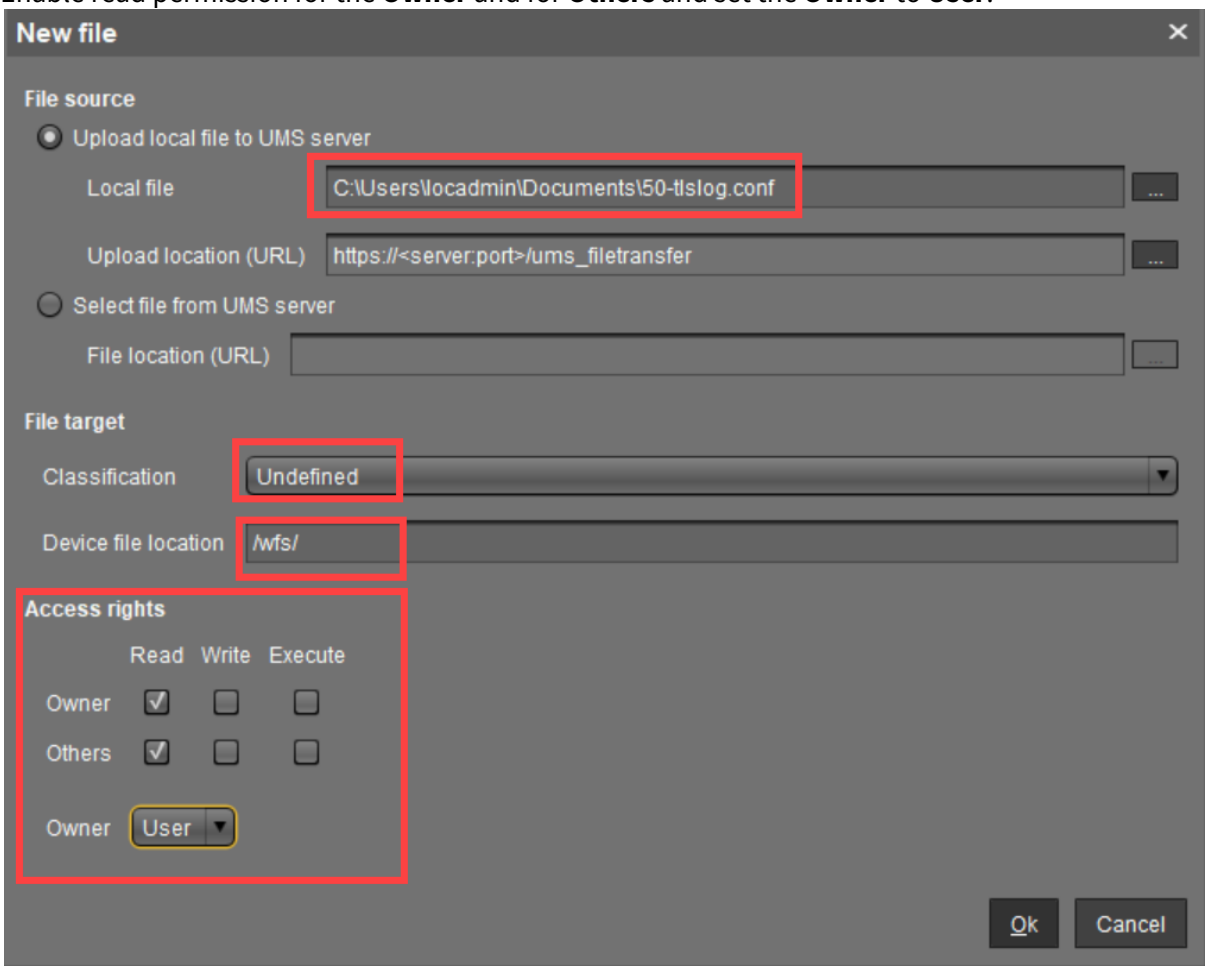


7. Save the changes and assign the profile to the desired devices.
8. Reboot the devices to make the change effective.

Instructions for IGEL OS before 11.06.100

In IGEL OS before version 11.06.100, configure the log forwarding with TLS encryption as follows:

1. Create a text file `50-tlslog.conf` with the following content:
   ```
   global(DefaultNetstreamDriverCAFile="/wfs/ca-certs/ca.pem")
   *.* action(type="omfwd" protocol="tcp"
   Target="<IP address or DNS name of the log collector>" port="<Port of the log collector)"
   StreamDriver="gtls" StreamDriverMode="1" StreamDriverAuthMode="anon"
   template="RSYSLOG_TraditionalFileFormat")
   ```
2. Create a **new file** in the UMS Console under **Files** by right-clicking.
3. Under **Local file**, select the file `50-tlslog.conf` and upload it.
4. Under **Classification**, select "Undefined".
5. Enter `/wfs/` under **Device file location**.
6. Enable read permission for the **Owner** and for **Others** and set the **Owner** to **User**.



7. Click **Ok**.
8. Assign the file object to the desired devices.
9. Create a profile with the following content:
   a. In the configuration dialog, go to **System > Firmware Customization > Custom Commands > Basic**.
   b. Enter the following line in the **Initialization** field:
   `cp /wfs/50-tlslog.conf /etc/rsyslog.d/`

10. Assign the profile to the desired devices.
11. Reboot the devices to make the change effective.

Action: Analyze Configuration Changes

In addition, various log entries for administrative activities can be searched in the Universal Management Suite:

- Choose **System > Logging > Log Messages** to see when settings and commands were sent to which device.
- Choose **System > Logging > Event Messages** to see changes to objects in the Universal Management Suite.
- Choose **System > Logging > Remote Access** to find out when which UMS user has shadowed which device using **Secure Shadowing**.

Datensicherung

This document is available in German only.

Verschlüsselung

Virenschutz

Systempflege

Zusätzliche Anforderungen aus SYS.2