Security & Safety

Exported on 10/26/2021

Table of Contents

1 IGEL Product Security Information

1.1 IGEL Security Notices (ISN)

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

1.2 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

1.2.1 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

1.2.2 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.

1.2.3 Update Instructions

- Update to UMS 6.08.120

1.2.4 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.

1.3 ISN 2021-06: IGEL OS OpenSSH Vulnerabilities

First published 2 August 2021

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

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

1.3.1 Summary

Three security vulnerabilities in OpenSSH affect the following IGEL products:

- IGEL OS 11
- IGEL OS 10

1.3.2 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).

1.3.3 Update Instructions

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

There are no updates yet for the other two issues.

1.3.4 Mitigation

- 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.
  - In IGEL Setup, go to **System > Remote Access > SSH Access**.
  - Uncheck the **Enable** checkbox.
  - Click **Apply**.
  - 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.

1.3.5 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

1.4 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

1.4.1 Summary

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

- IGEL OS 11
- IGEL OS 10

1.4.2 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).

1.4.3 Update Instructions

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

1.4.4 Mitigation

- Disable terminal access for the user, see Disabling Local Terminal Access[1].
- Disable virtual console access, see Disabling Virtual Console Access[2].
- 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[3].
  - Remove the Mobile Device Access USB feature (removed by default), see Removing Unused Features[4].

1.4.5 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

1.5 ISN 2021-04: IGEL OS Kernel Privilege Escalation

Announced 23 July 2021

1 https://kb.igel.com/display/igelos1105/Disabling+Local+Terminal+Access
2 https://kb.igel.com/display/igelos1105/Disabling+Virtual+Console+Access
3 https://kb.igel.com/display/igelos1105/Disabling+Storage+Hotplug
4 https://kb.igel.com/display/igelos1105/Removing+Unused+Features

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

1.5.1 Summary

A local privilege escalation vulnerability affects the following IGEL products:

- IGEL OS 11
- IGEL OS 10

1.5.2 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.

1.5.3 Update Instructions

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

1.5.4 Mitigation

- Disable terminal access for the user, see Disabling Local Terminal Access[5].
- Disable virtual console access, see Disabling Virtual Console Access[6].
- 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[7].
  - Remove the Mobile Device Access USB feature (removed by default), see Removing Unused Features[8].
- 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

1.5.5 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

5 https://kb.igel.com/display/igelos1105/Disabling+Local+Terminal+Access
6 https://kb.igel.com/display/igelos1105/Disabling+Virtual+Console+Access
7 https://kb.igel.com/display/igelos1105/Disabling+Storage+Hotplug
8 https://kb.igel.com/display/igelos1105/Removing+Unused+Features

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

1.6 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

1.6.1 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.

1.6.2 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.

1.6.3 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

1.7 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

1.7.1 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[9]: Aggregation attack (accepting non-SPP A-MSDU frames)
- CVE-2020-24587[10]: Mixed key attack (reassembling fragments encrypted under different keys)
- CVE-2020-24586[11]: 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[12]: Accepting plaintext data frames in a protected network
- CVE-2020-26143[13]: Accepting fragmented plaintext data frames in a protected network

Other implementation flaws are assigned the following CVEs:

- CVE-2020-26147[14]: Reassembling mixed encrypted/plaintext fragments
- CVE-2020-26141[15]: Not verifying the TKIP MIC of fragmented frames.

9 https://nvd.nist.gov/vuln/detail/CVE-2020-24588
10 https://nvd.nist.gov/vuln/detail/CVE-2020-24587
11 https://nvd.nist.gov/vuln/detail/CVE-2020-24586
12 https://nvd.nist.gov/vuln/detail/CVE-2020-26140
13 https://nvd.nist.gov/vuln/detail/CVE-2020-26143
14 https://nvd.nist.gov/vuln/detail/CVE-2020-26147
15 https://nvd.nist.gov/vuln/detail/CVE-2020-26141

1.7.2 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.

1.7.3 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.

1.7.4 References

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

1.8 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

1.8.1 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.

1.8.2 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.

1.8.3 Mitigation

Disable secure shadowing, see Shadow[16]. However, it is not advisable to use unencrypted shadowing instead.

Disable secure terminal, see Secure Terminal[17].

1.9 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

1.9.1 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.

1.9.2 Update Instructions

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

1.9.3 Mitigation

Disable Bluetooth, see Bluetooth Assistant[18].

1.9.4 References

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

16 https://kb.igel.com/display/igelos1104/Shadow
17 https://kb.igel.com/display/igelos1104/Secure+Terminal
18 https://kb.igel.com/display/igelos1104/Bluetooth+Assistant

1.10 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)

1.10.1 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.

1.10.2 Update Instructions

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

1.10.3 Mitigation

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

1.11 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

1.11.1 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).

1.11.2 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

1.11.3 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/

1.12 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

1.12.1 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).

1.12.2 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[19].

19 https://kb.igel.com/display/igellinux/Features

1.12.3 References

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

1.13 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.

1.13.1 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.

1.13.2 Update Instructions

- Update to IGEL Cloud Gateway 2.02.100 or newer.

1.14 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)

1.14.1 Details

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

1.14.2 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

1.14.3 References

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

1.15 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

1.15.1 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).

1.15.2 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

1.15.3 References

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

1.16 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

1.16.1 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.

1.16.2 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

1.16.3 References

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

1.17 ISN 2020-02: Windows CryptoAPI Spoofing Vulnerability

Announced 24 February 2020

Score: High

A high scoring security issue affects IGEL Windows 10 IoT

1.17.1 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".

1.17.2 Update Instructions

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

1.17.3 References

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

1.18 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

1.18.1 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).

1.18.2 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

1.18.3 References

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

1.19 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

1.19.1 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.

1.19.2 Update Instructions

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

1.19.3 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

1.20 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

1.20.1 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.

1.20.2 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.

1.20.3 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

1.21 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

1.21.1 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.

1.21.2 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

1.21.3 References

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

1.22 ISN 2019-10: Spectre SWAPGS CPU Vulnerability

Announced 16 August 2019

Score: Low

A security issue affects Intel and AMD x86_64 CPUs.

1.22.1 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.

1.22.2 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.

1.22.3 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

1.23 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

1.23.1 Details

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

1.23.2 Update Instructions

- Update to IGEL OS 10.06.110 or newer.

1.24 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

1.24.1 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.

1.24.2 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.

1.24.3 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

1.24.4 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/

1.25 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

1.25.1 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.

1.25.2 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.

1.25.3 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

1.26 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

1.26.1 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.

1.26.2 Update Instructions

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

1.26.3 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`

1.26.4 References

Advisory from Netflix with further suggestions for workarounds:

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

1.27 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

1.27.1 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.

1.27.2 Update Instructions

Update to UMS 6.02.100 or newer.

To update your UMS installation, please follow these instructions: Updating UMS[20]

1.28 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.

1.28.1 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.

1.28.2 Update Instructions

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

1.28.3 Further Information

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

1.29 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

20 https://kb.igel.com/display/endpointmgmt602/Updating+UMS

1.29.1 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.

1.29.2 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)

1.30 ISN 2019-02: UMS Vulnerability

1.30.1 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

1.30.2 Details

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

1.30.3 Update Instructions

UMS 6.x

Update to UMS 6.01.130 or newer. For instructions, see Updating UMS[21].

21 https://kb.igel.com/display/endpointmgmt601/Updating+UMS

UMS 5.x

Update to UMS 5.09.140 or newer. For instructions, see Updating UMS[22].

1.31 ISN 2019-01: UMS Vulnerability

1.31.1 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

1.31.2 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.

1.31.3 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[23]

22 https://kb.igel.com/display/endpointmgmt509/Updating+UMS
23 https://kb.igel.com/display/endpointmgmt601/Updating+UMS

2 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[24]

IGEL Meltdown and Spectre (2)
Notice from 2018-02-01
Security fixes available for download[25]
See newsletter[26]

IGEL Meltdown and Spectre
Notice from 2018-01-18
Security fixes available for download[27]
See newsletter[28]

KRACK Attacks
Notice from 2017-10-23
Security fixes available for download[29]
See newsletter[30]

24 https://kb.igel.com/display/igelos/SSH%3A+Deprecation+of+Weak+Algorithms+as+of+IGEL+Linux+10.04.100
25 https://www.igel.com/software-downloads/
26 https://mailchi.mp/6ede7858d1c2/igel-technical-newsletter-january18_meltdown_spectre-1289945
27 https://www.igel.com/software-downloads/
28 http://mailchi.mp/6d07867522c2/igel-technical-newsletter-january18_meltdown_spectre-1289889
29 https://www.igel.com/software-downloads/
30 http://mailchi.mp/b68f2468dce3/igel-technical-newsletter-august-1289593

3 Reporting Vulnerabilities

Have you discovered a security vulnerability in an IGEL product?

Please contact security@igel.com[31] to report it. A PGP/GPG key for confidential communication is available upon request.

31 mailto:security@igel.com

4 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 35)
- UD3-LX 50 (see page 42)
- UD3-LX 51 (see page 48)
- UD6-LX 51 (see page 54)
- UD7-LX 10 (see page 61)
- UD3-W10 51 (see page 64)
- UD6-W10 51 (see page 70)
- UD7-W10 10 (see page 77)

4.1 IGEL OS

4.1.1 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[32] corresponds to *BayTrail.5.04.32.0022* or higher.

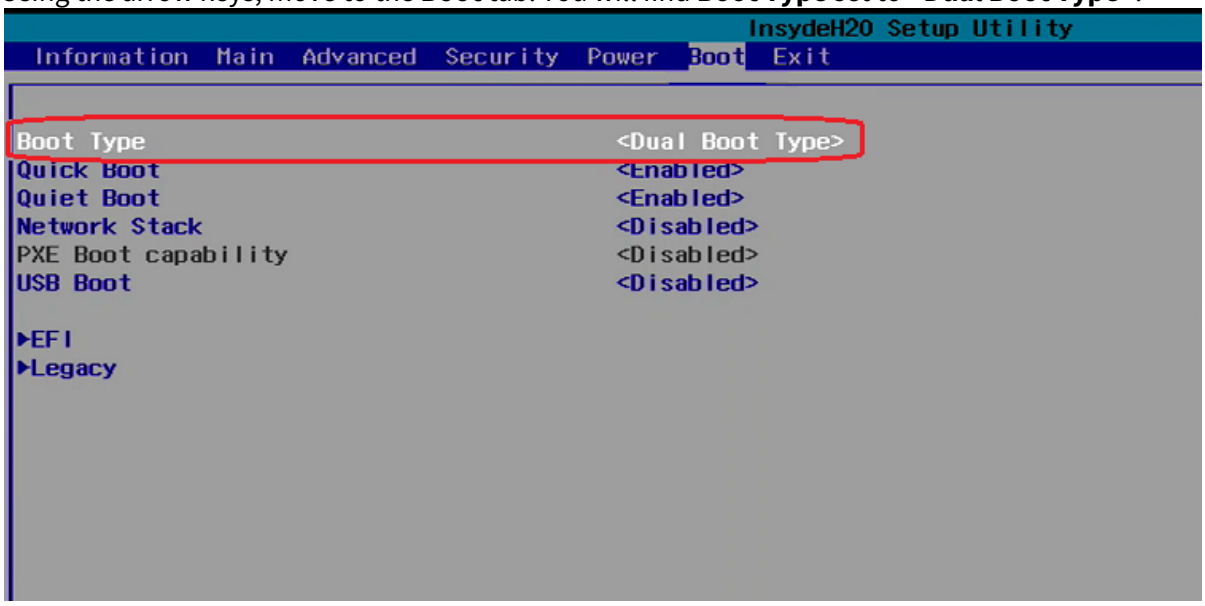
It is crucial to set a BIOS password to prevent users from disabling Secure Boot.

32 https://kb.igel.com/display/hardware/How+Can+I+Update+the+BIOS+Version

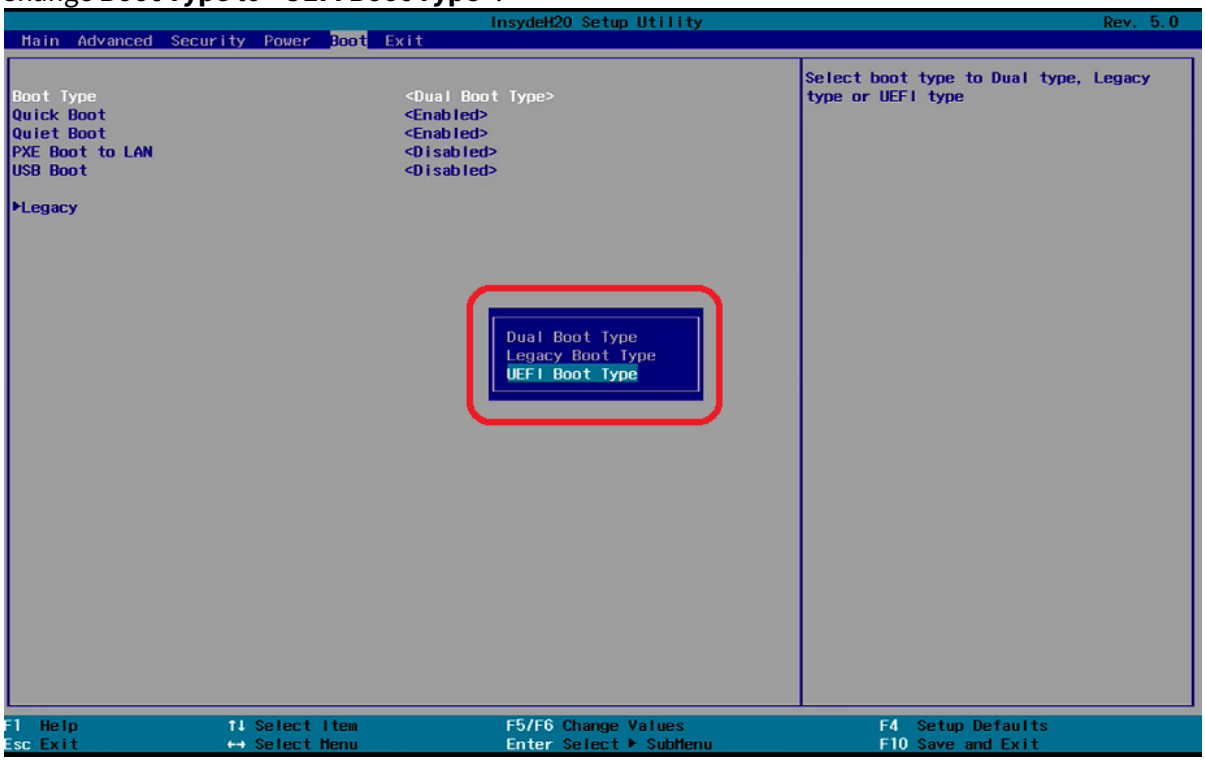
Changing the Device's Boot Type to UEFI Boot

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.

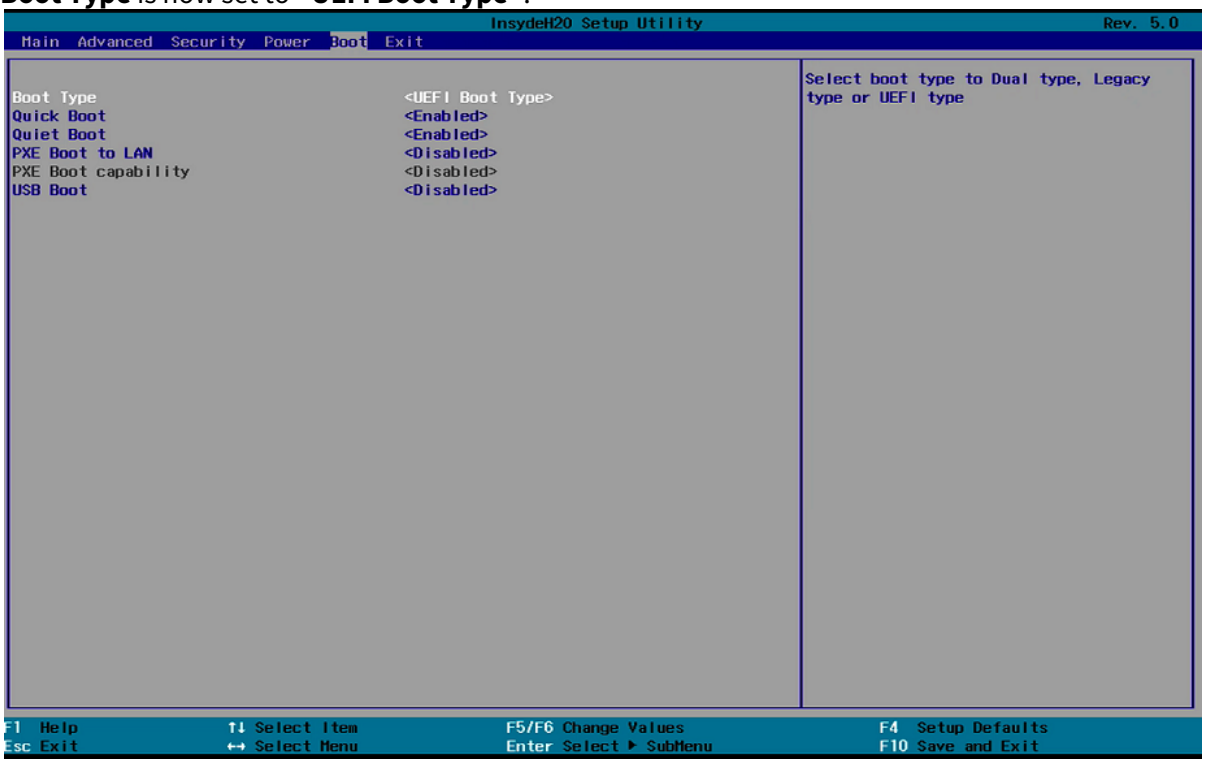
4. Using the arrow keys, move to the **Boot** tab. You will find **Boot Type** set to **<Dual Boot Type>**.



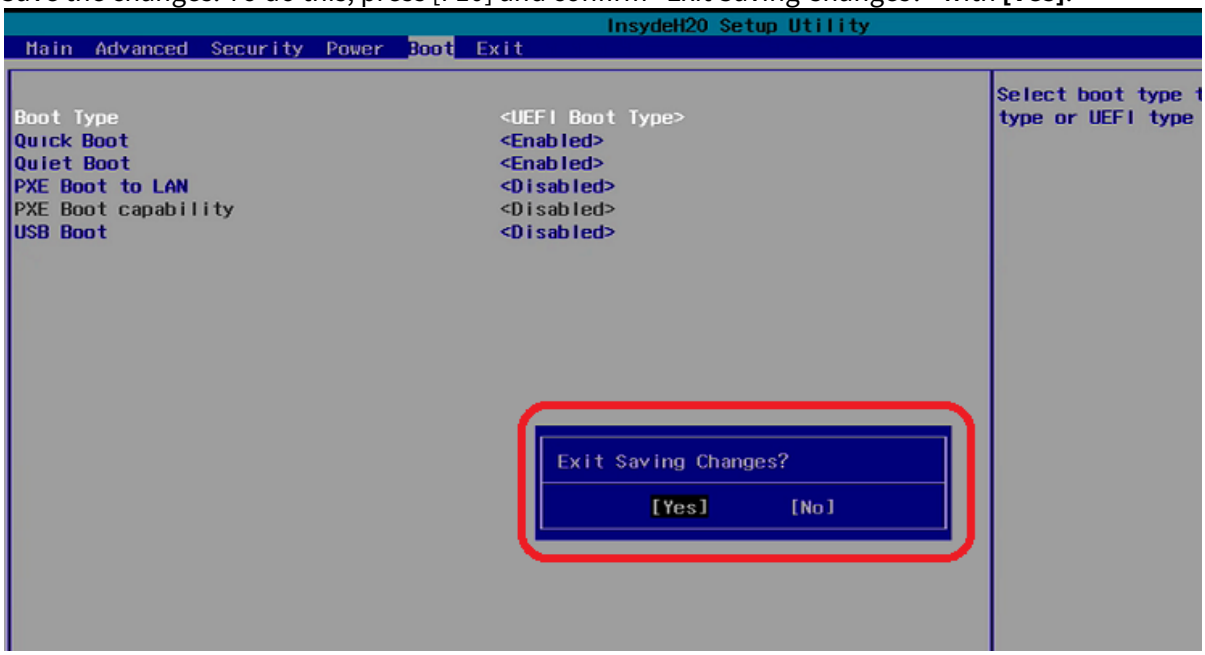
5. Change **Boot Type** to **<UEFI Boot Type>**.



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]**.

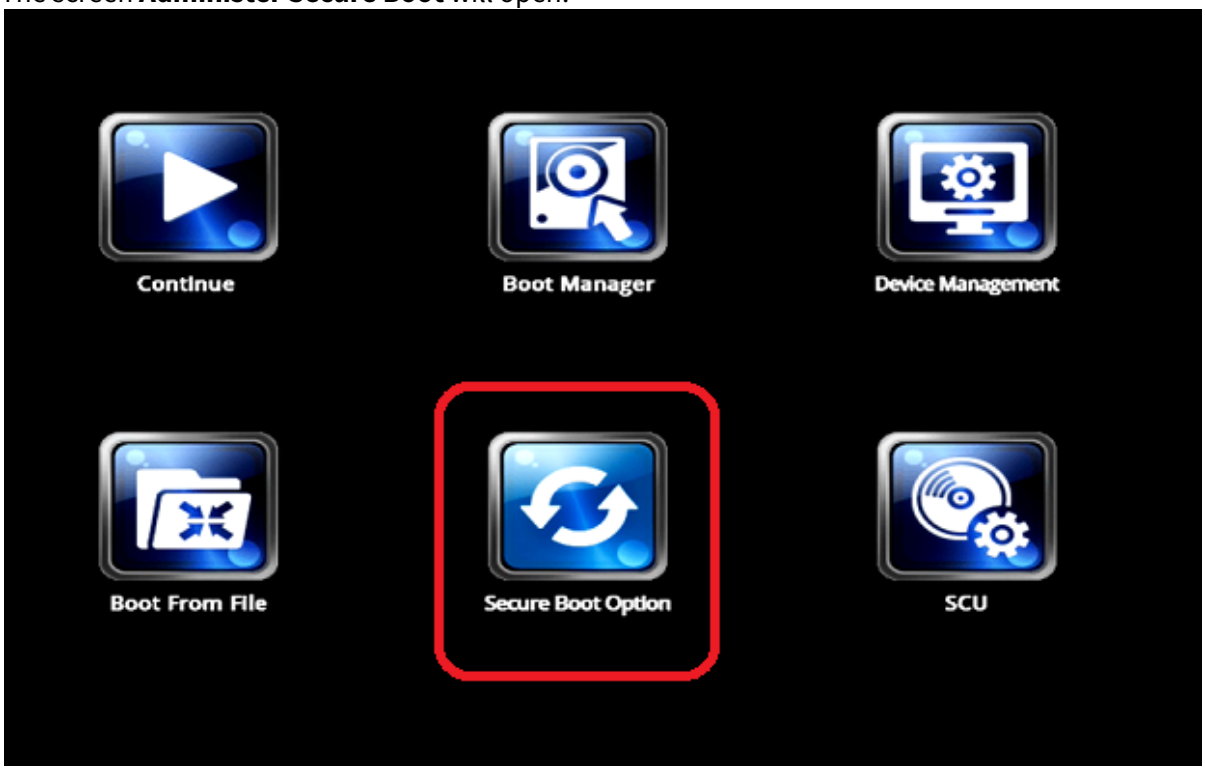


The settings are now saved and the device is rebooted.

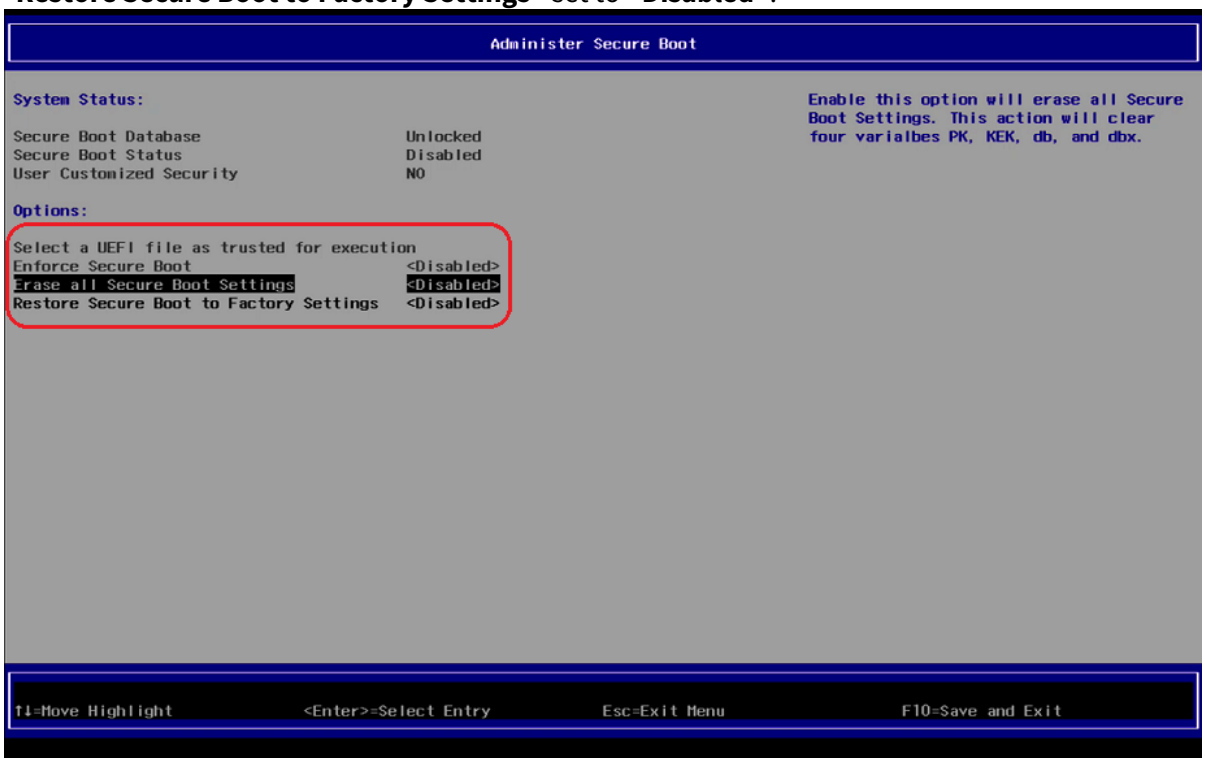
Activating the Secure Boot Feature

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.

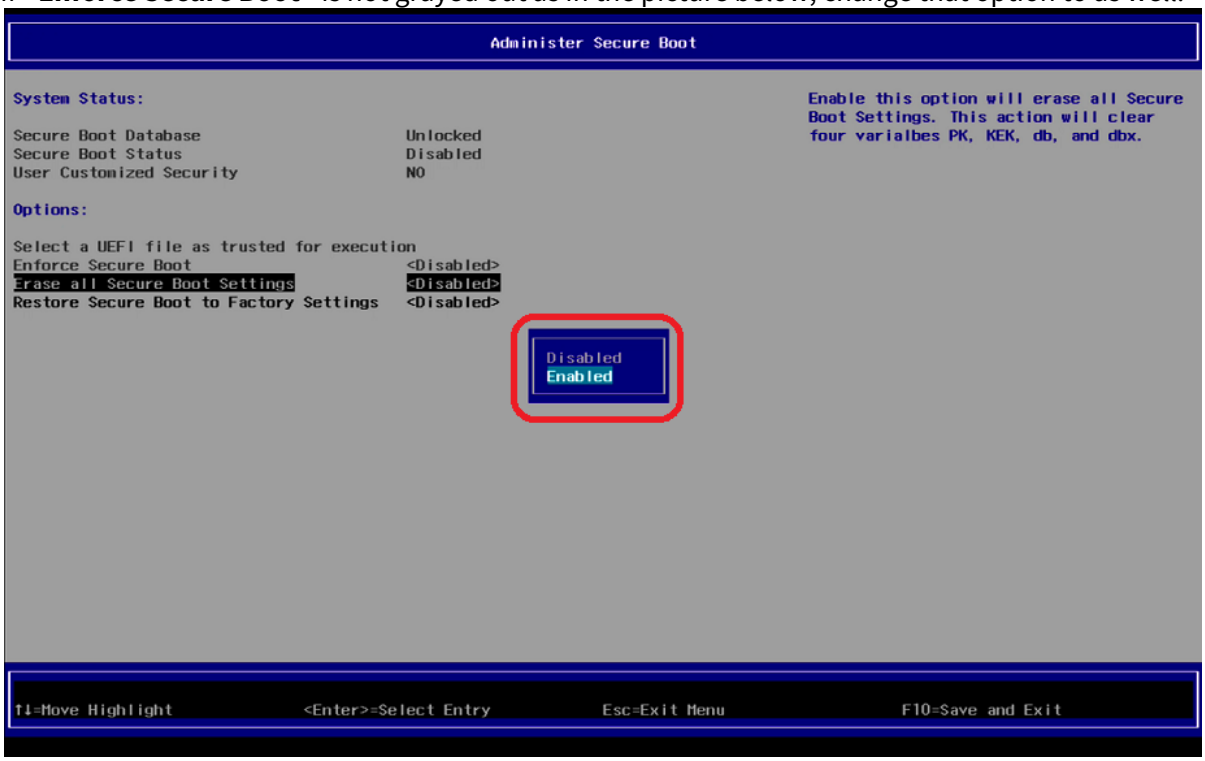


4. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.

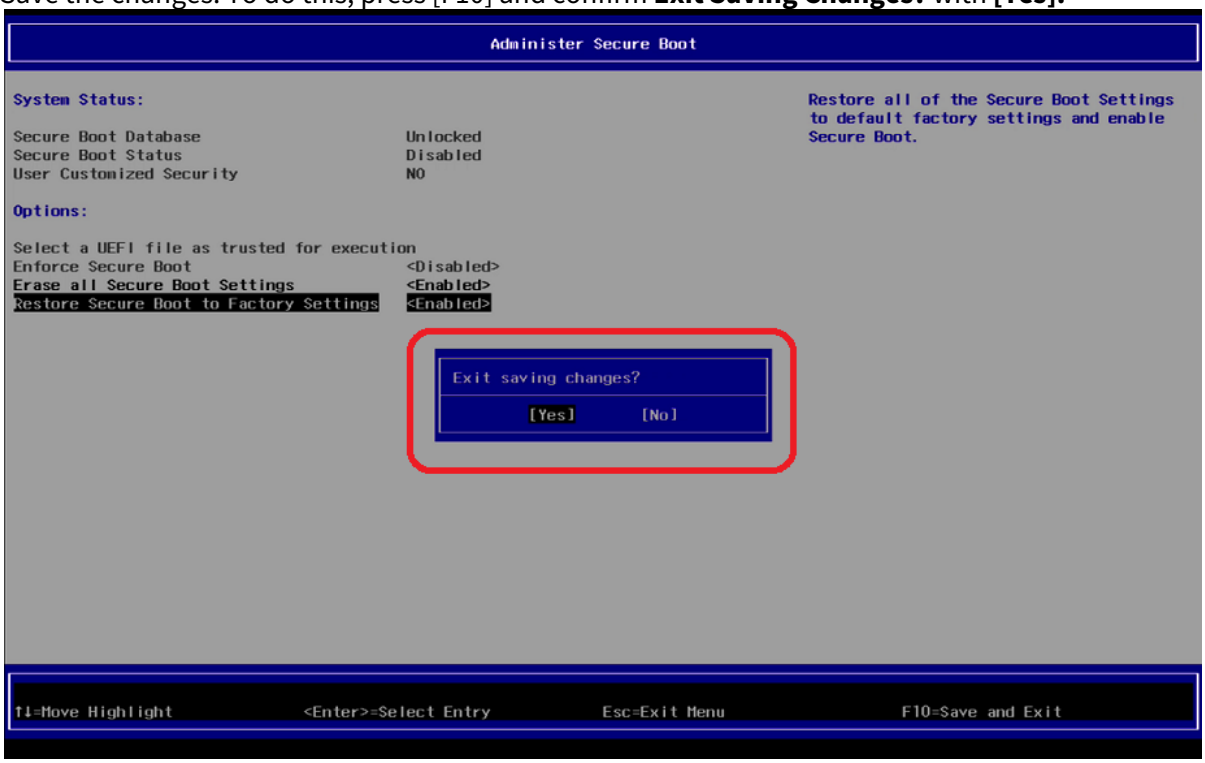


5. Change **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.

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[33].

4.1.2 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.

4.1.3 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[34] corresponds to *3.A. 13-11202017* or higher.

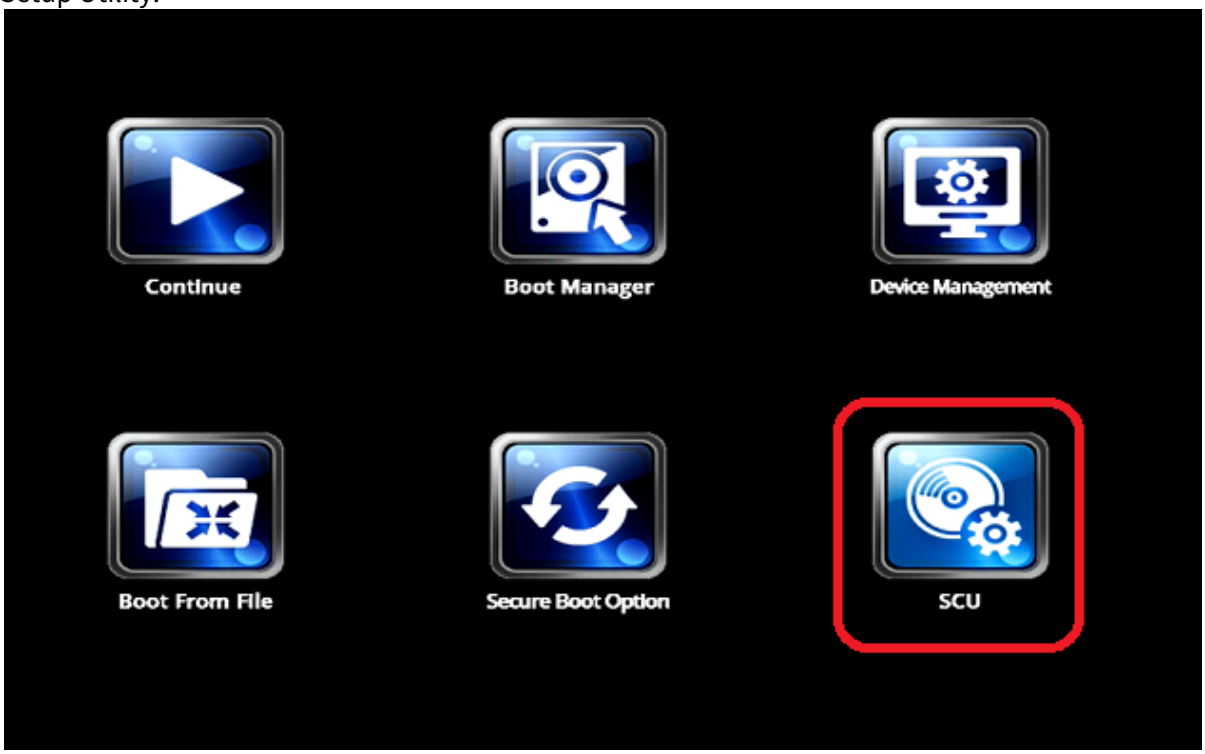
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Changing the Device's Boot Type to UEFI Boot

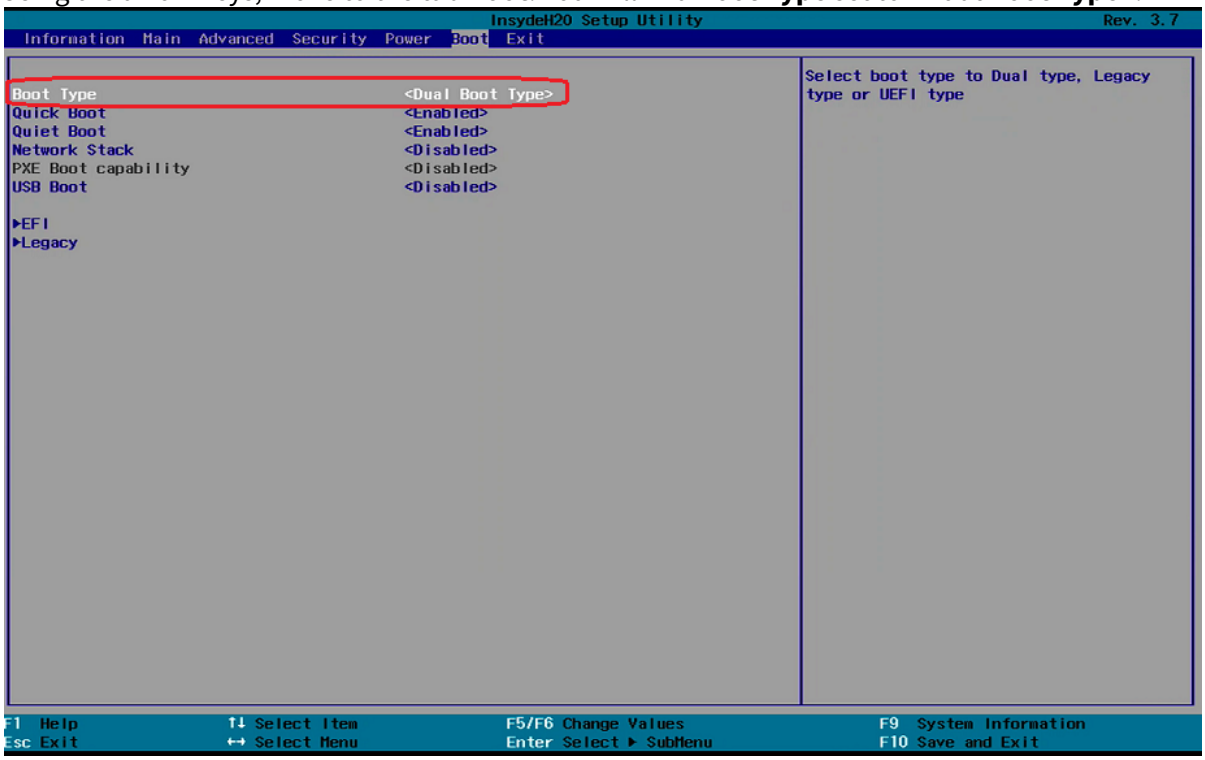
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.

33 https://kb.igel.com/display/securitysafety/Veryfing+that+UEFI+Secure+Boot+is+enabled
34 https://kb.igel.com/display/hardware/How+Can+I+Update+the+BIOS+Version

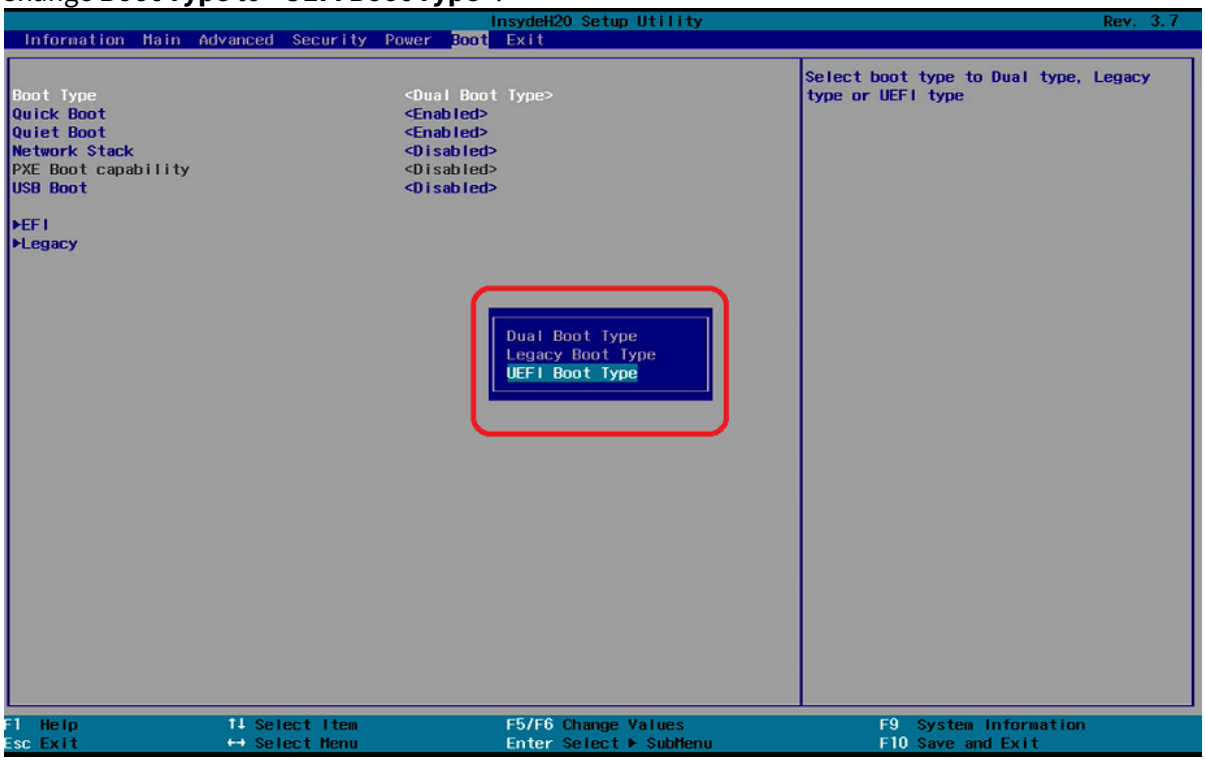
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



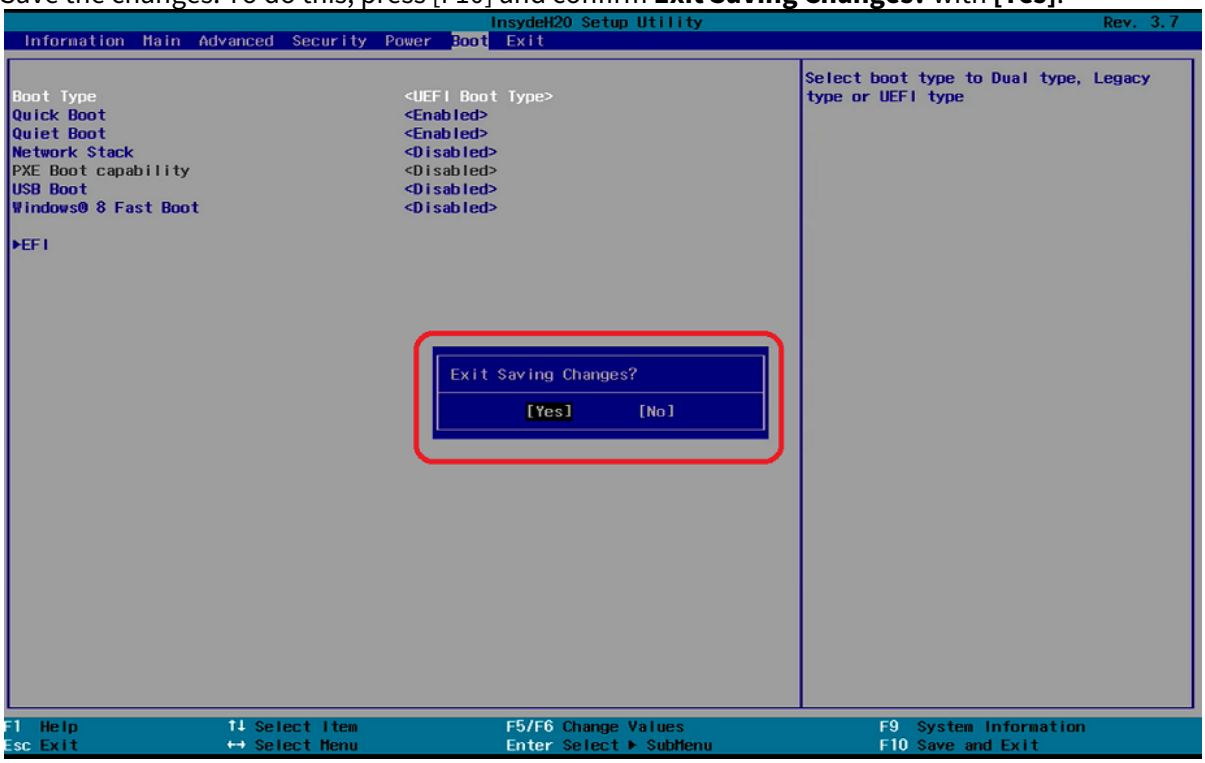
4. Using the arrow keys, move to the tab **Boot**. You will find **Boot Type** set to **<Dual Boot Type>**.



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



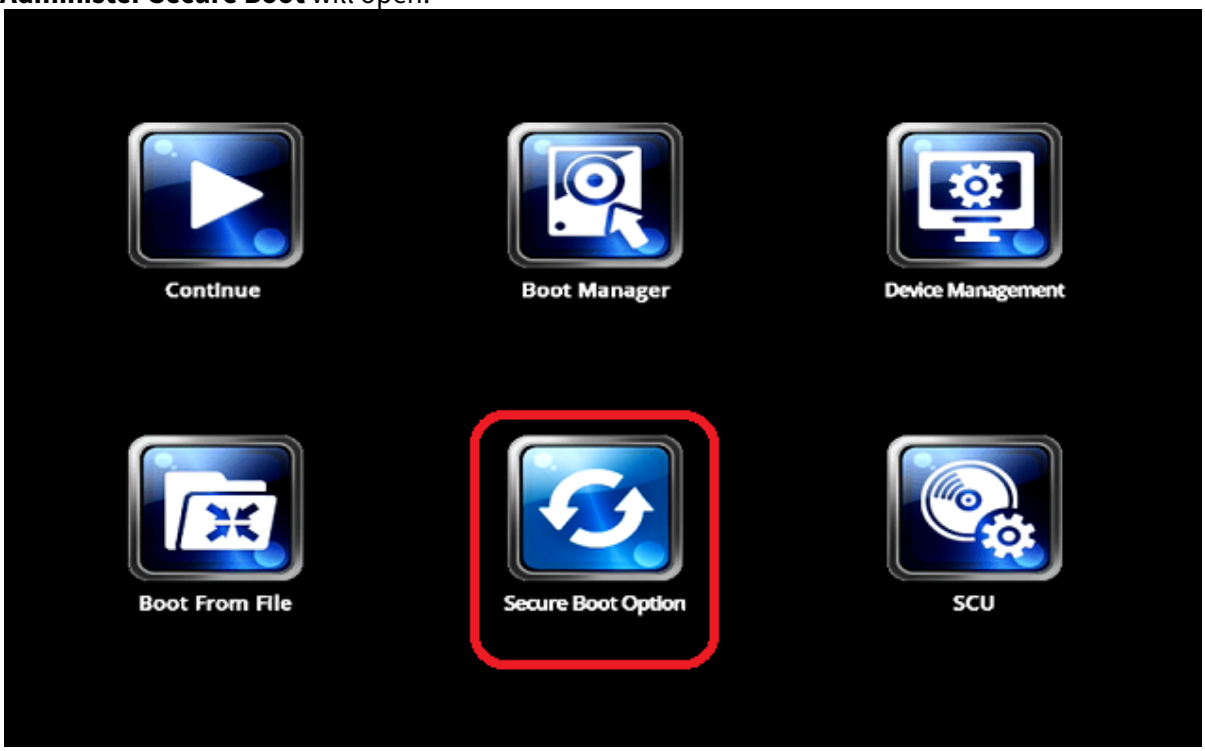
6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.



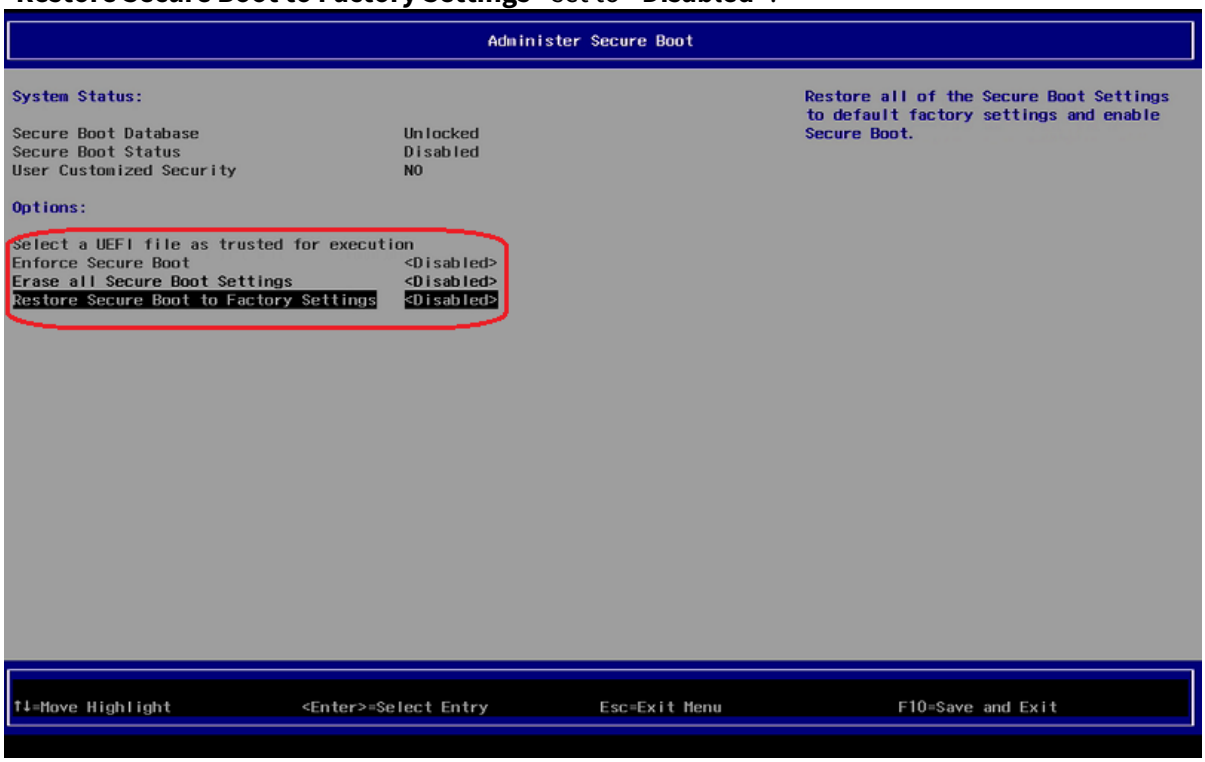
The changes will be saved and the device will be rebooted.

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.

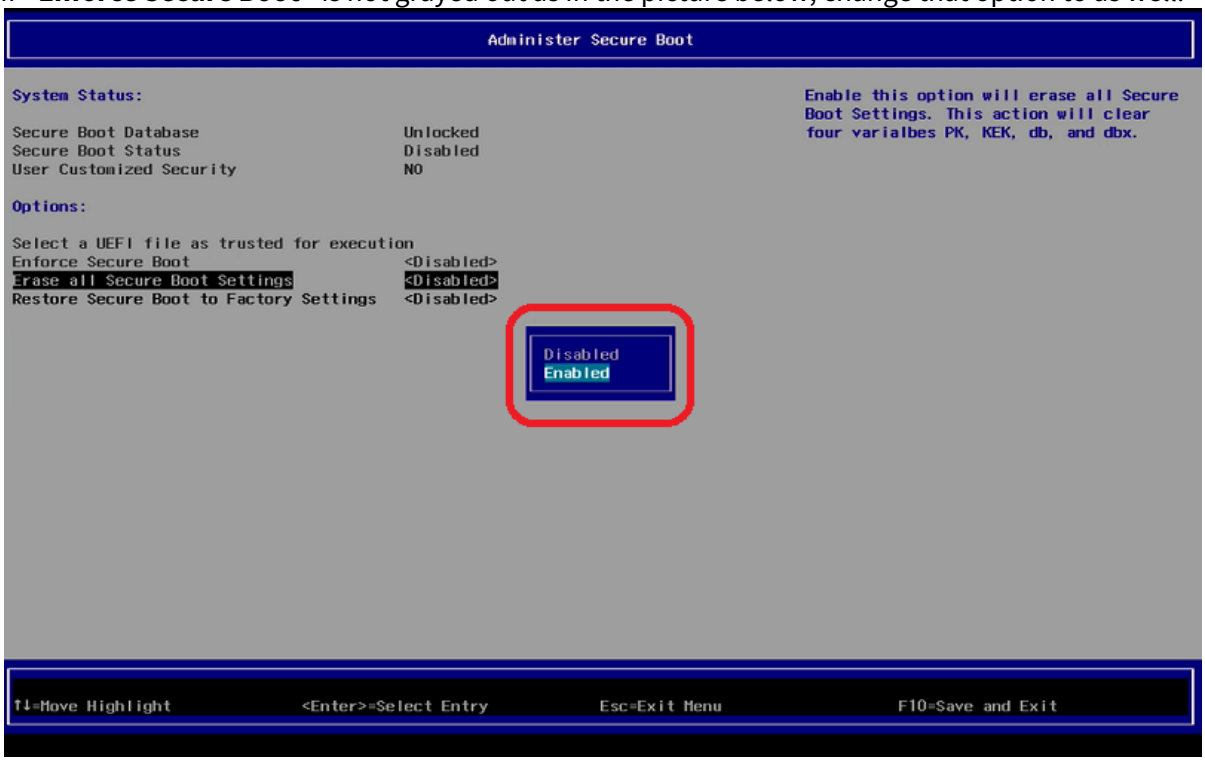


3. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.

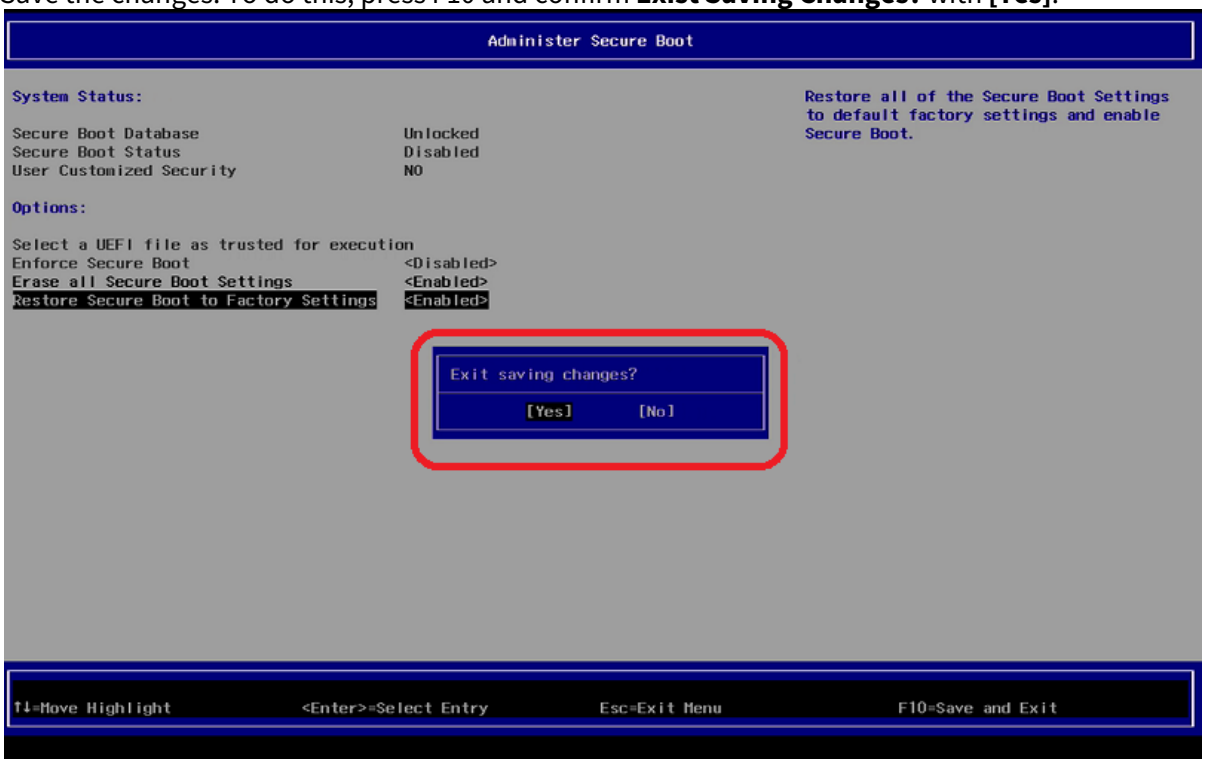


4. Change **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.

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[35].

4.1.4 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[36] corresponds to *3.A. 13-11202017* or higher.

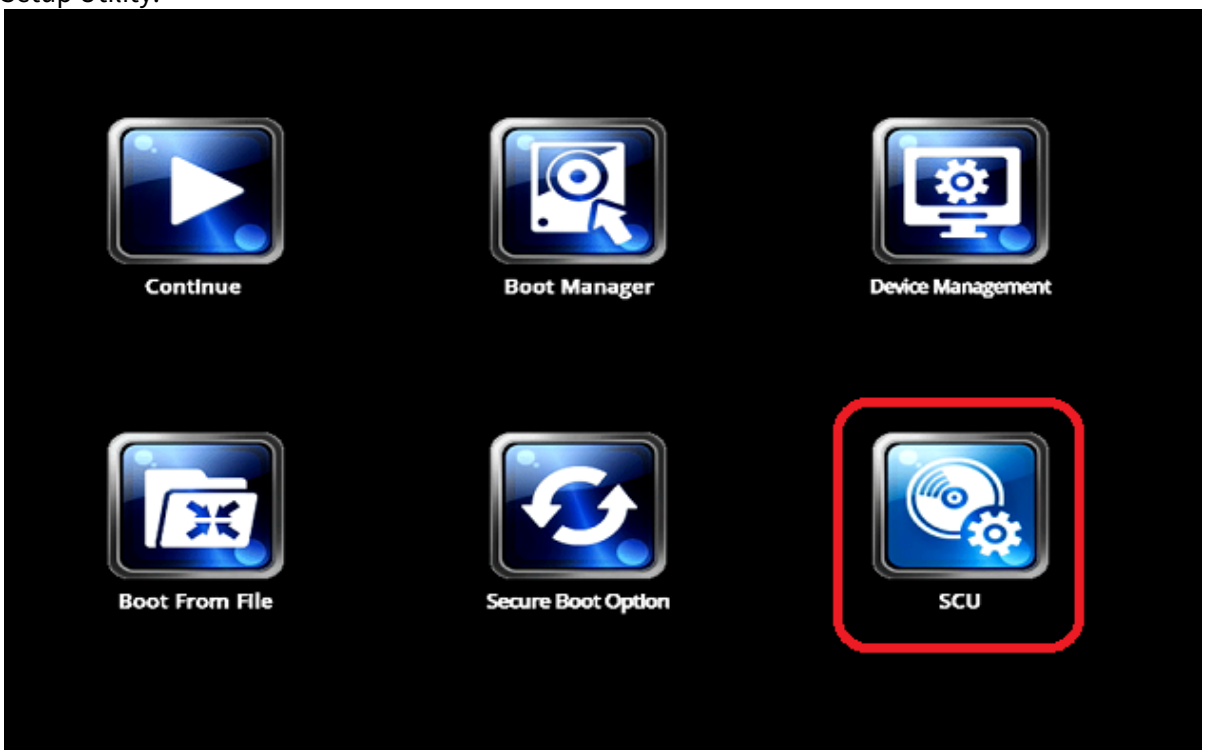
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Changing the Device's Boot Type to UEFI Boot

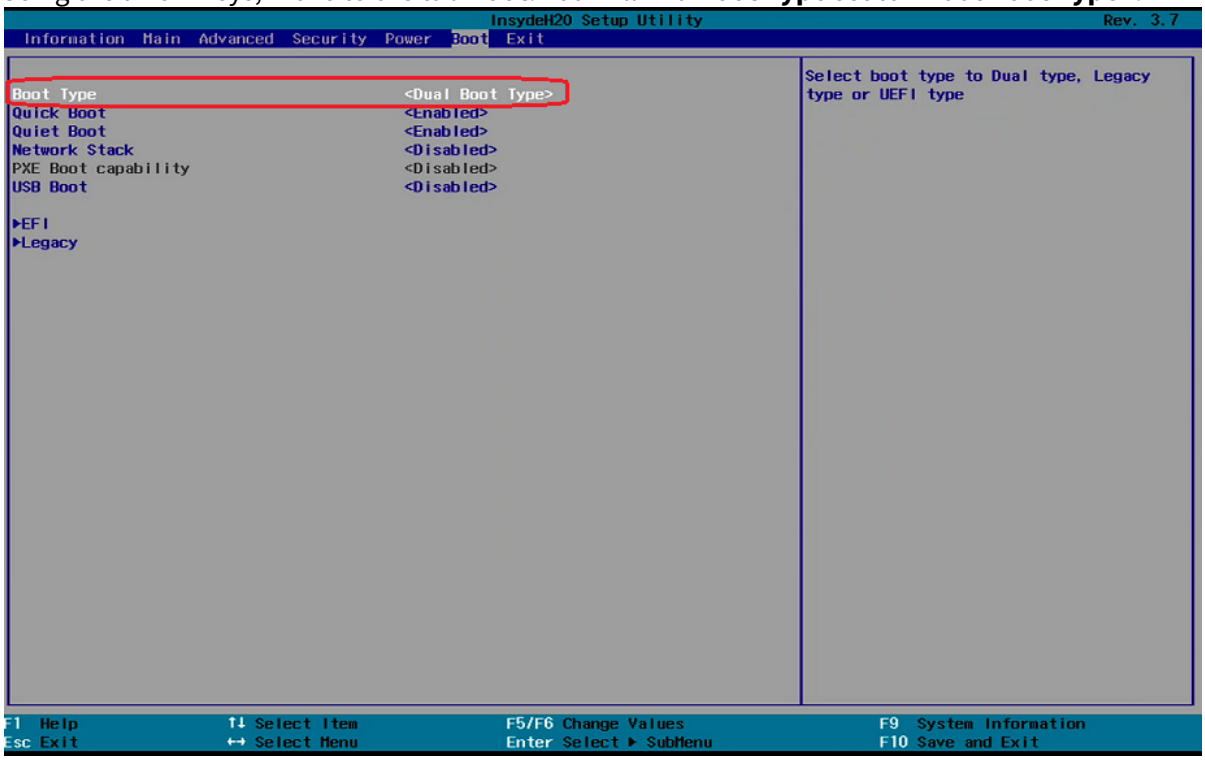
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.

35 https://kb.igel.com/display/securitysafety/Veryfing+that+UEFI+Secure+Boot+is+enabled
36 https://kb.igel.com/display/hardware/How+Can+I+Update+the+BIOS+Version

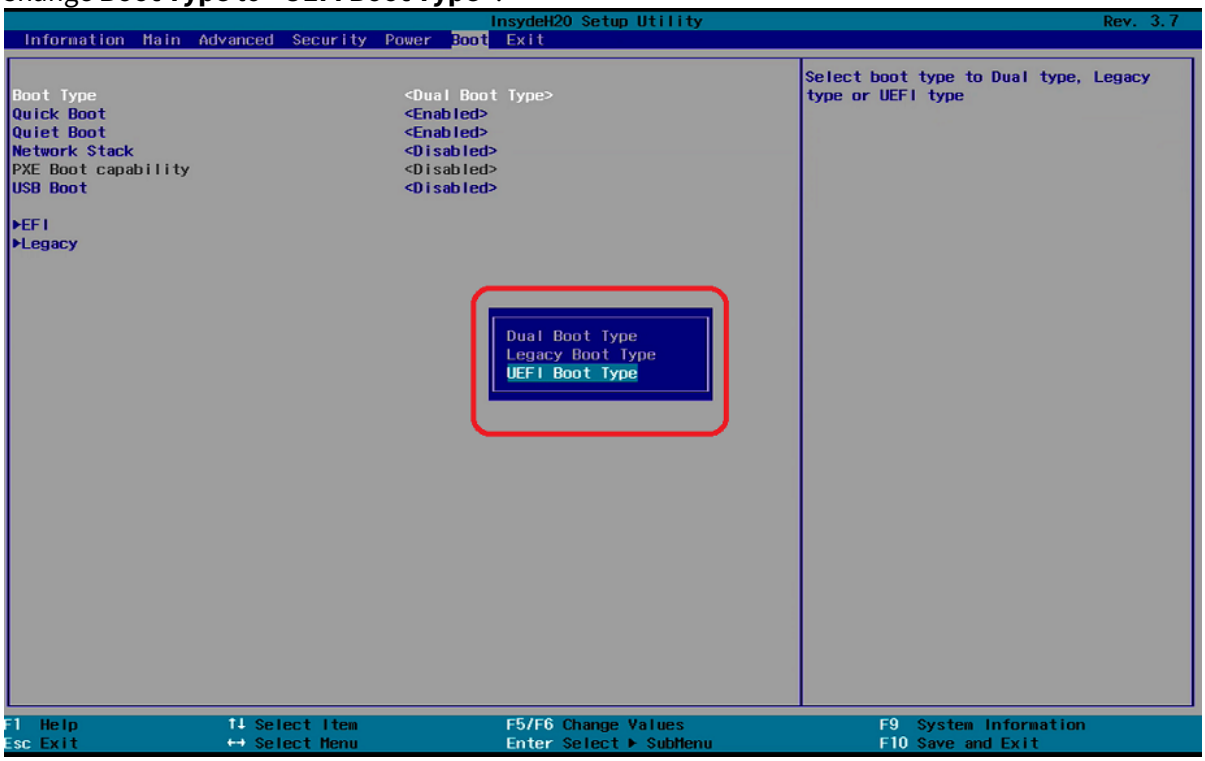
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



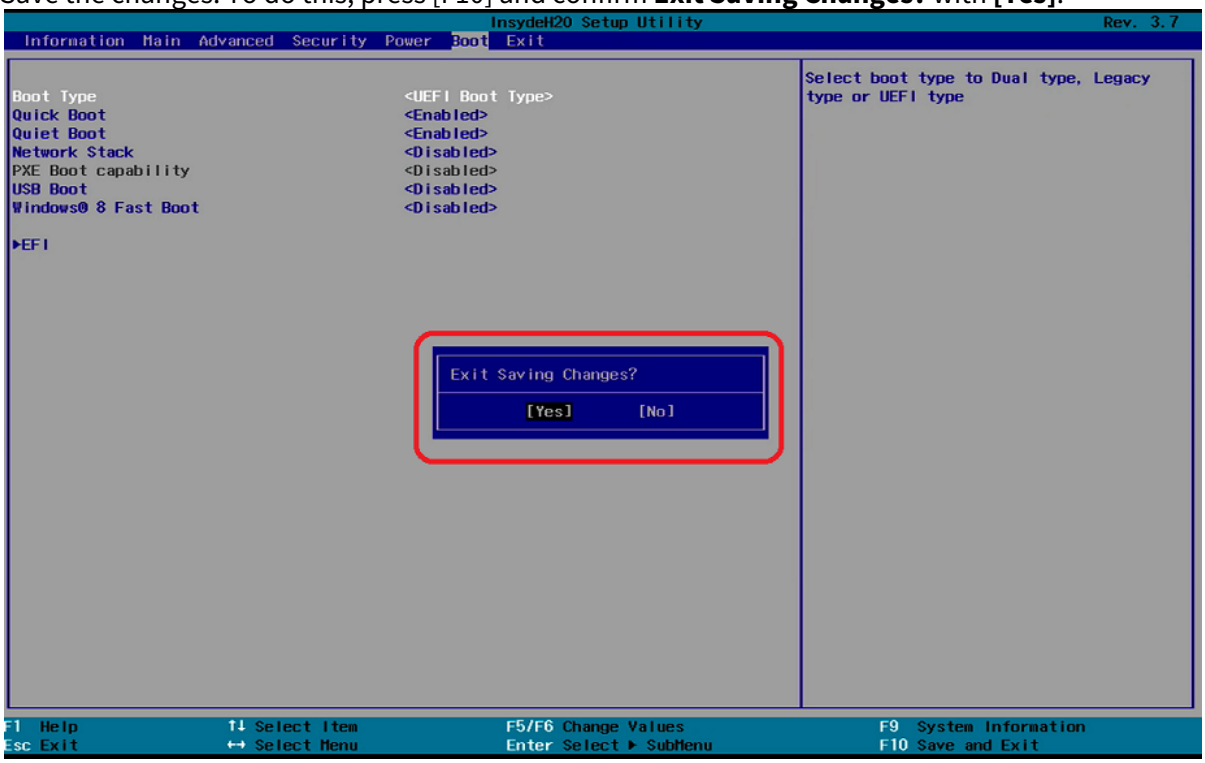
4. Using the arrow keys, move to the tab **Boot**. You will find **Boot Type** set to **<Dual Boot Type>**.



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



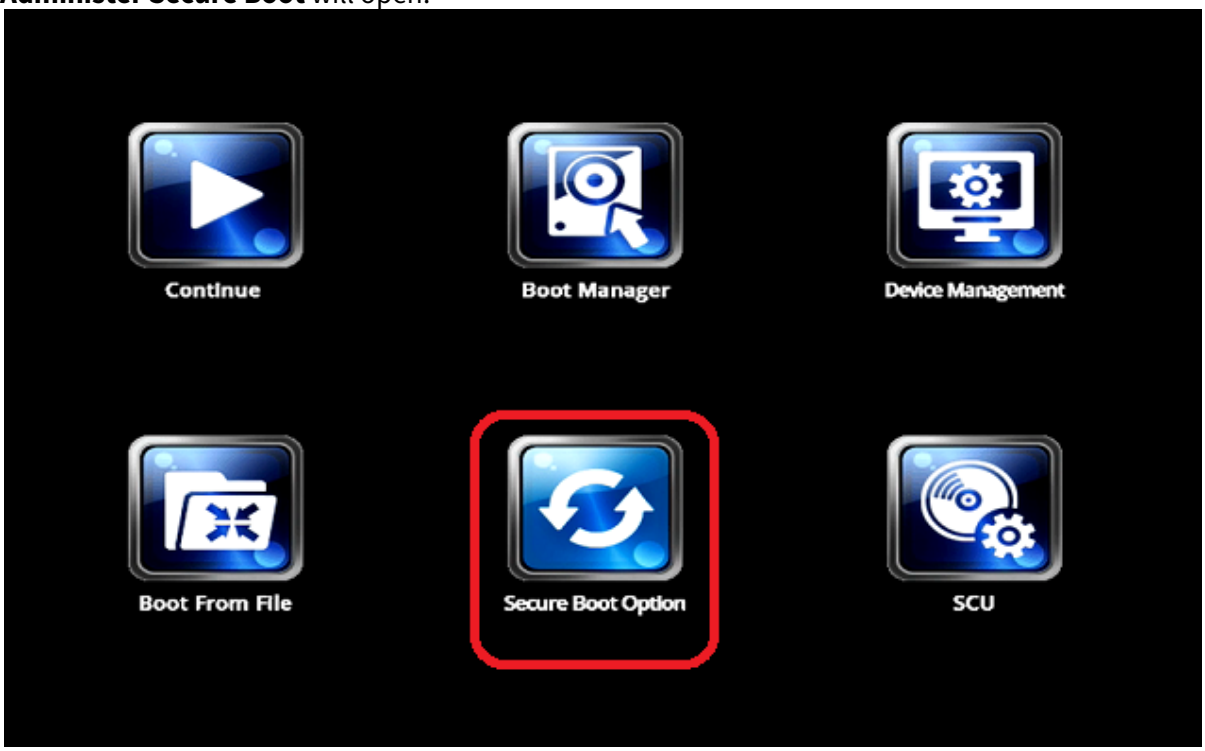
6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.



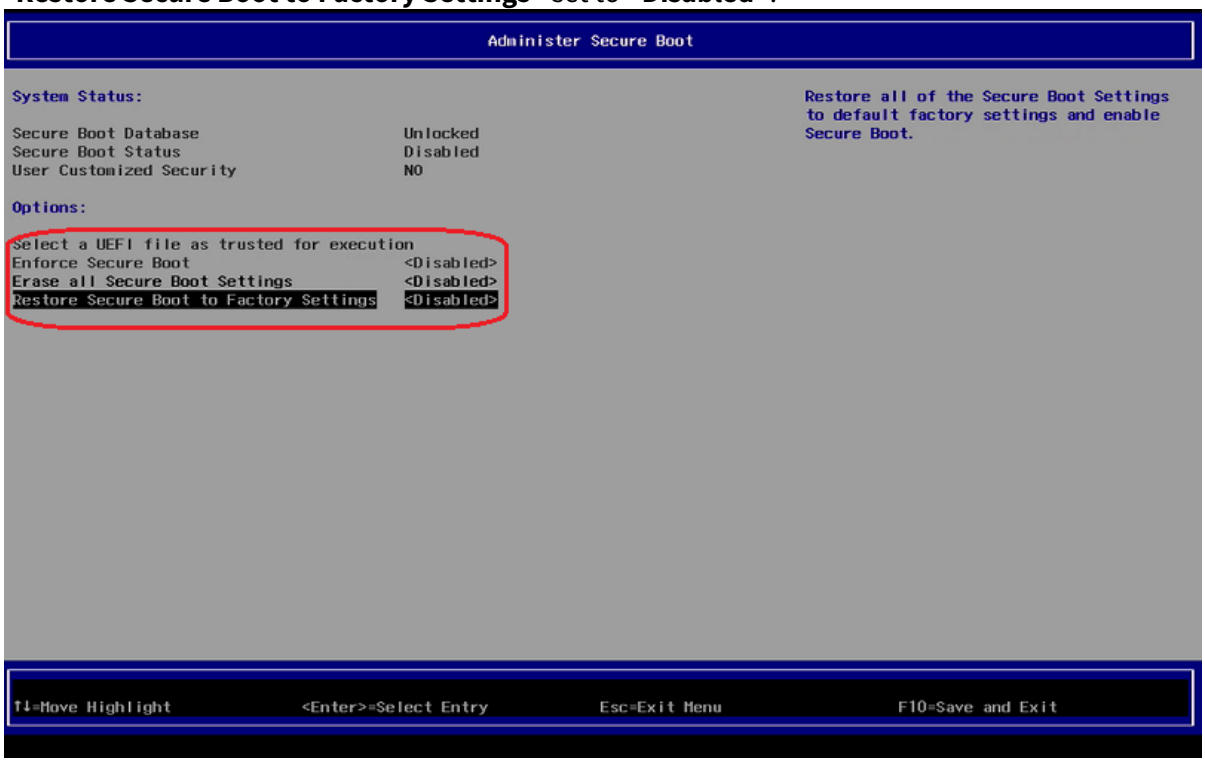
The changes will be saved and the device will be rebooted.

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.

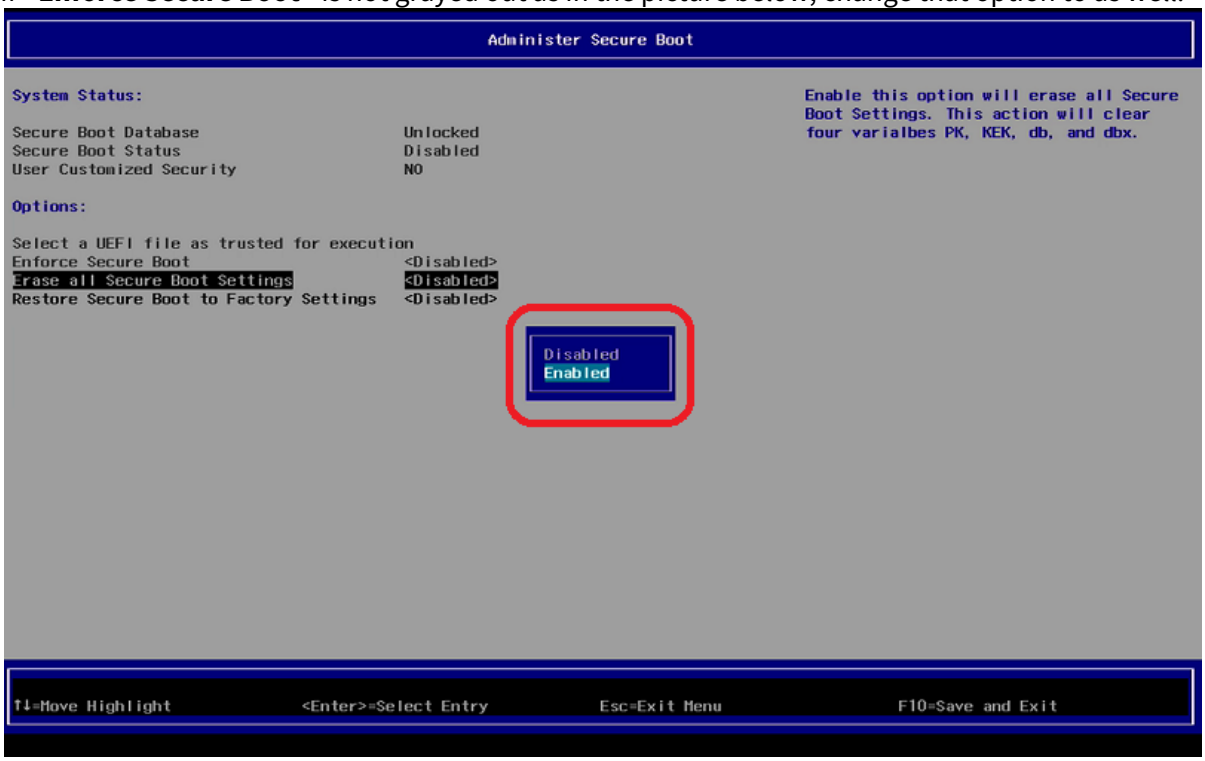


3. In the screen **Administer Secure Boot**, you will find **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** set to **<Disabled>**.

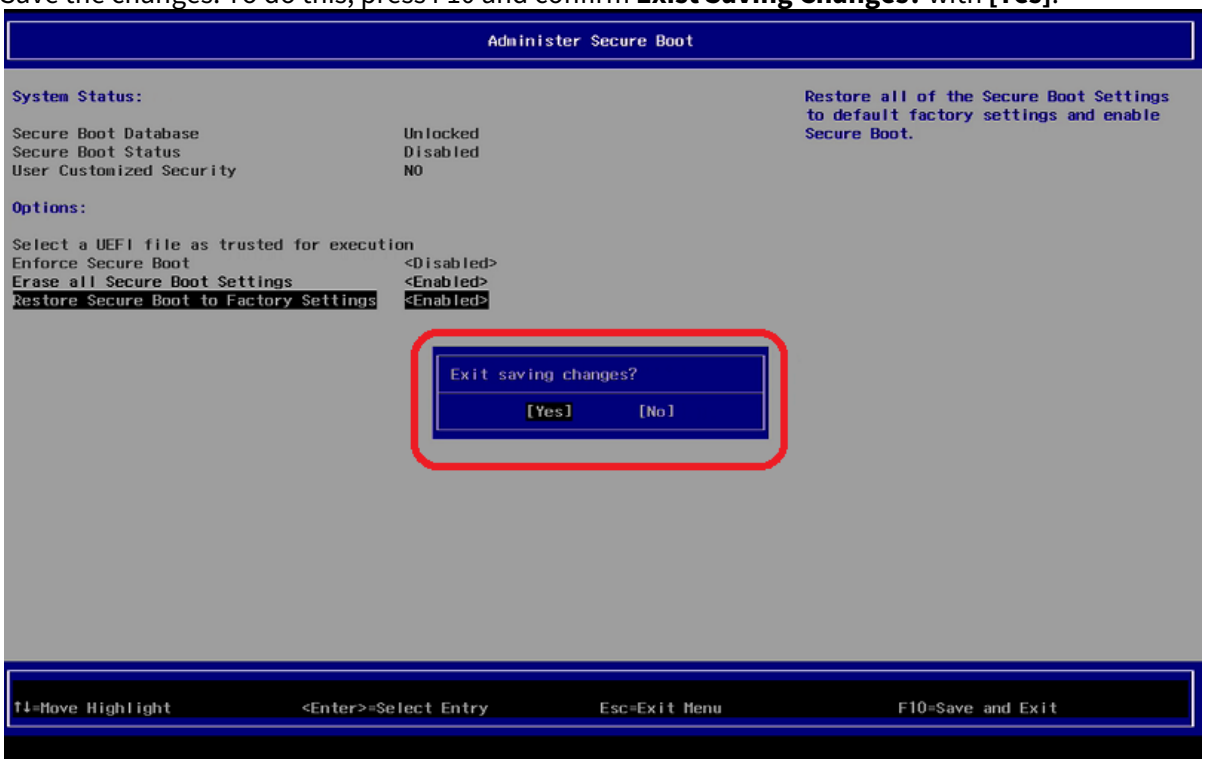


4. Change **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.

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[37].

4.1.5 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.

4.1.6 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[38] corresponds to *3.9. 13-02202017* or newer.

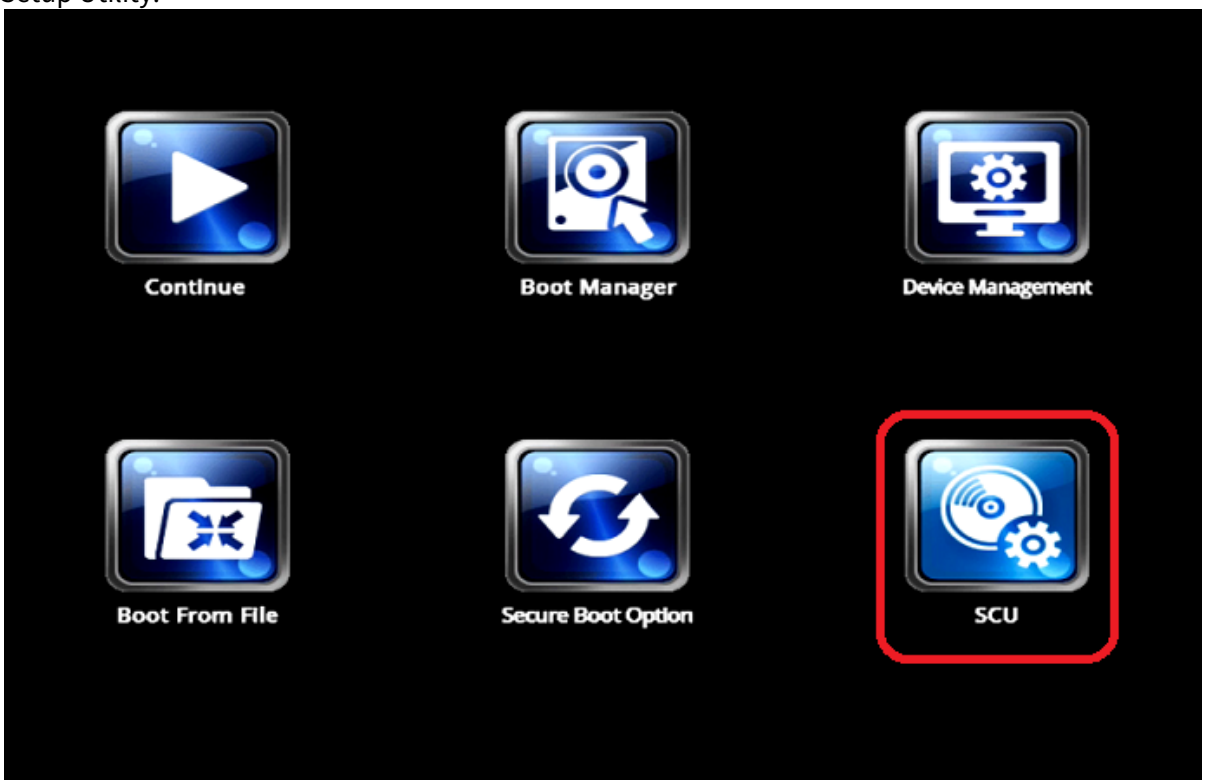
It is crucial to set a BIOS password to prevent users from disabling Secure Boot.

Changing the Device's Boot Type to UEFI Boot

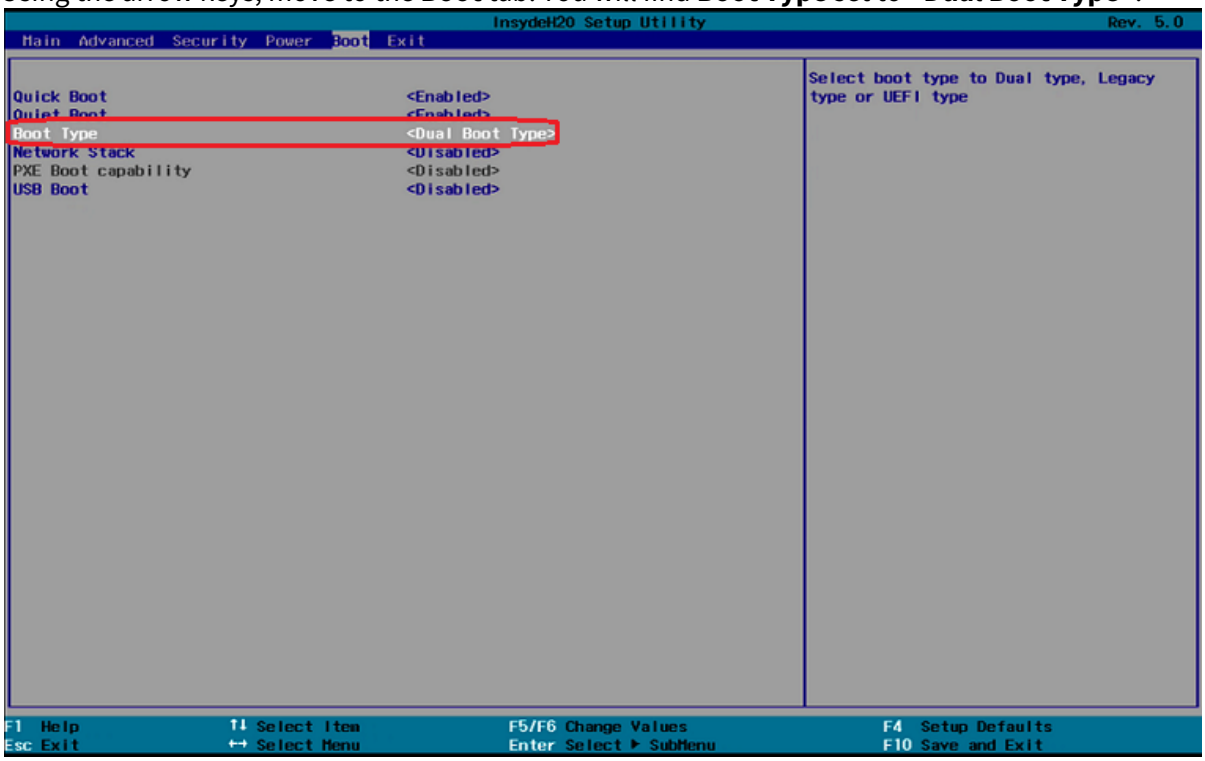
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.

37 https://kb.igel.com/display/securitysafety/Veryfing+that+UEFI+Secure+Boot+is+enabled
38 https://kb.igel.com/display/hardware/How+Can+I+Update+the+BIOS+Version

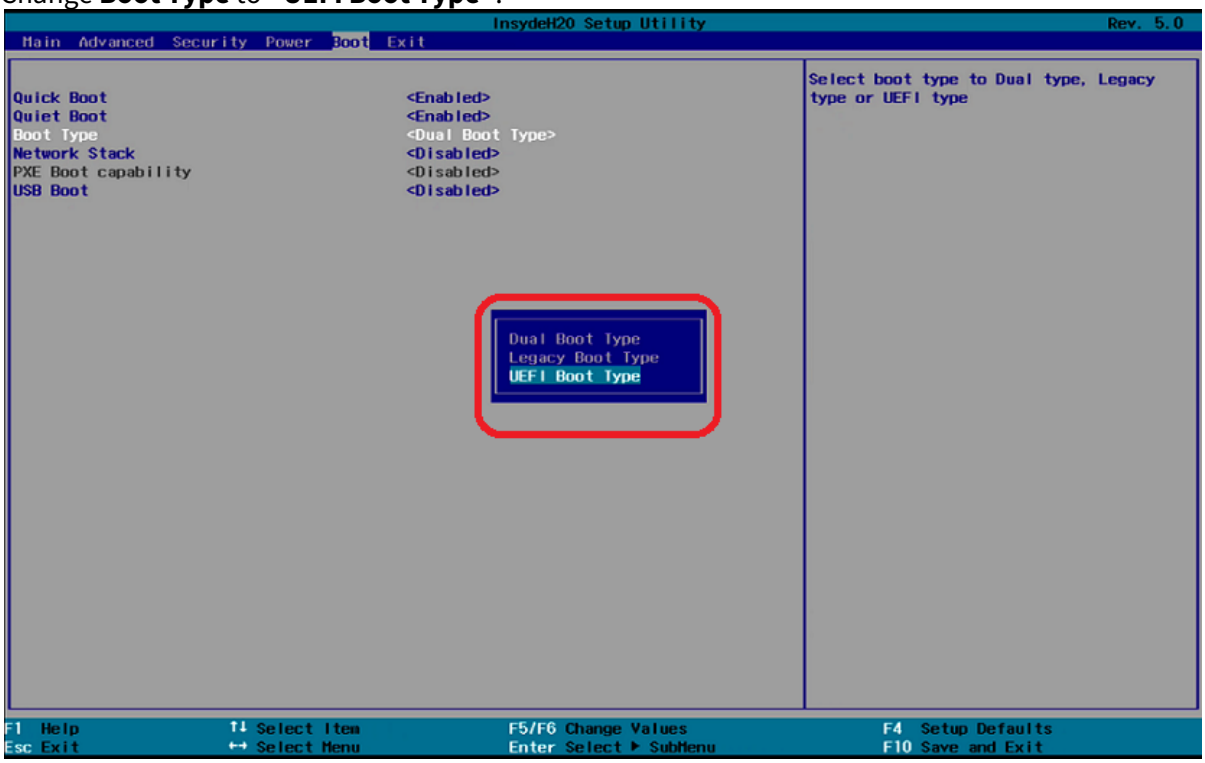
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



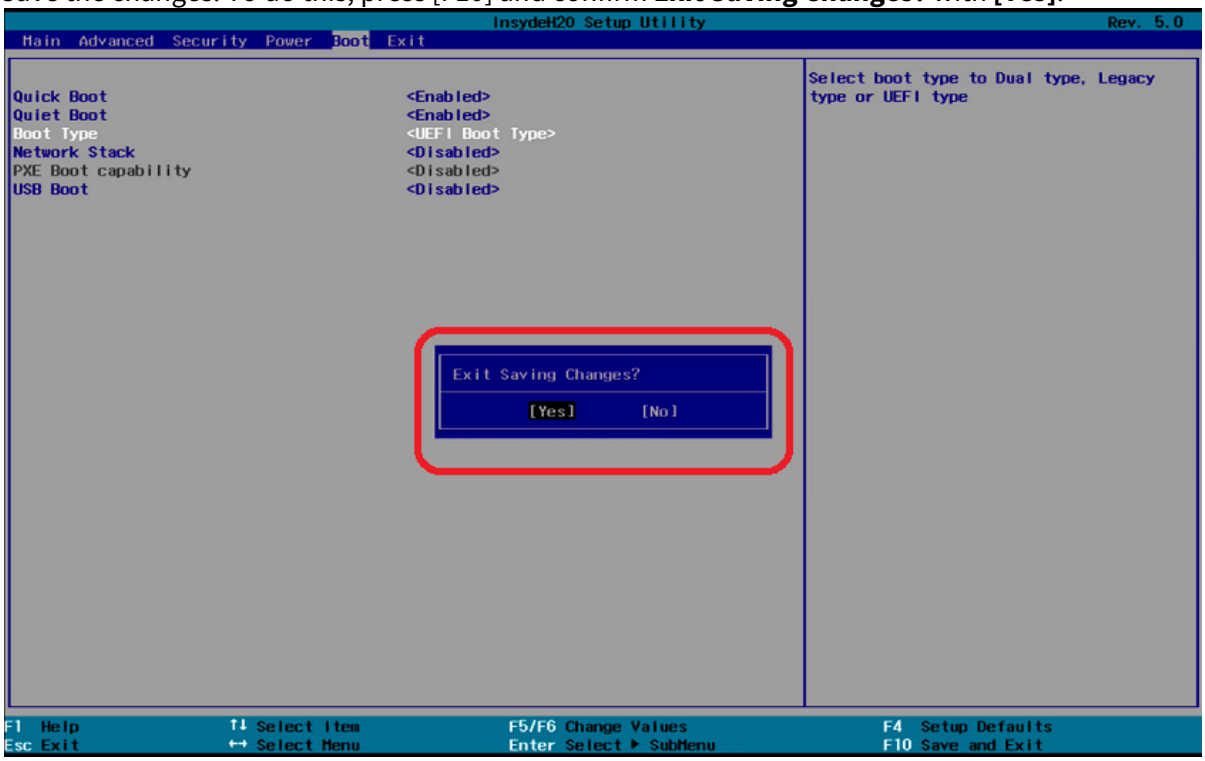
4. Using the arrow keys, move to the **Boot** tab. You will find **Boot Type** set to **<Dual Boot Type>**.



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



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

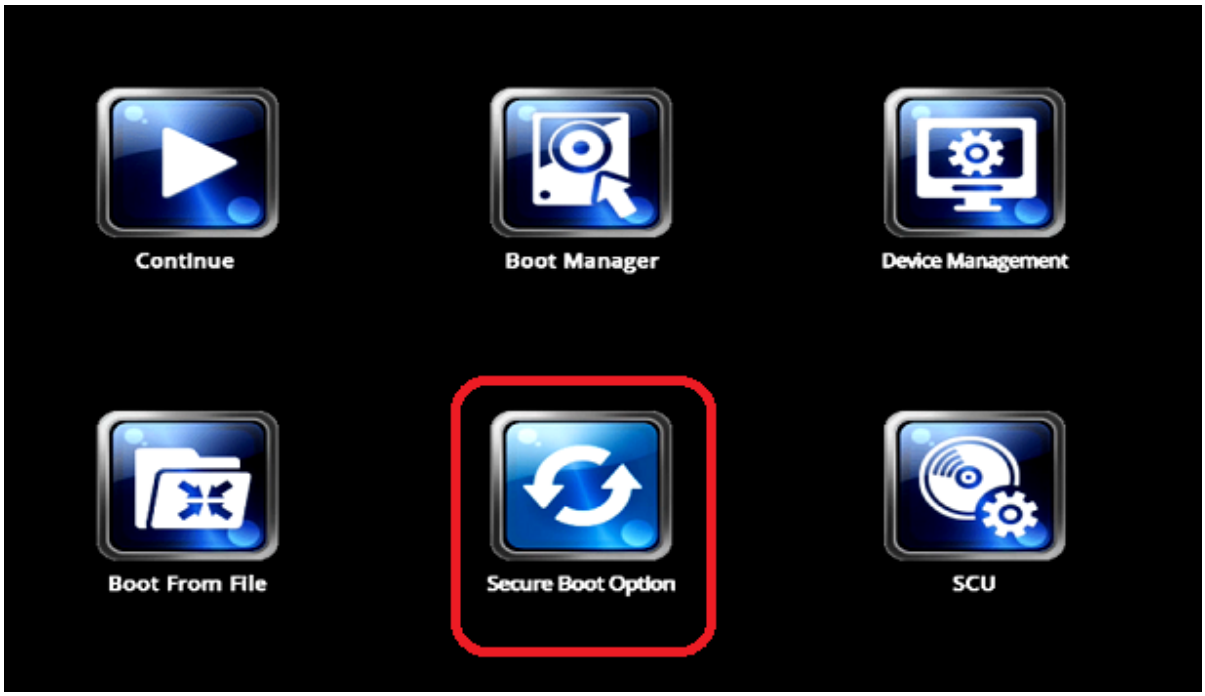


The changes will be saved and the device will be rebooted.

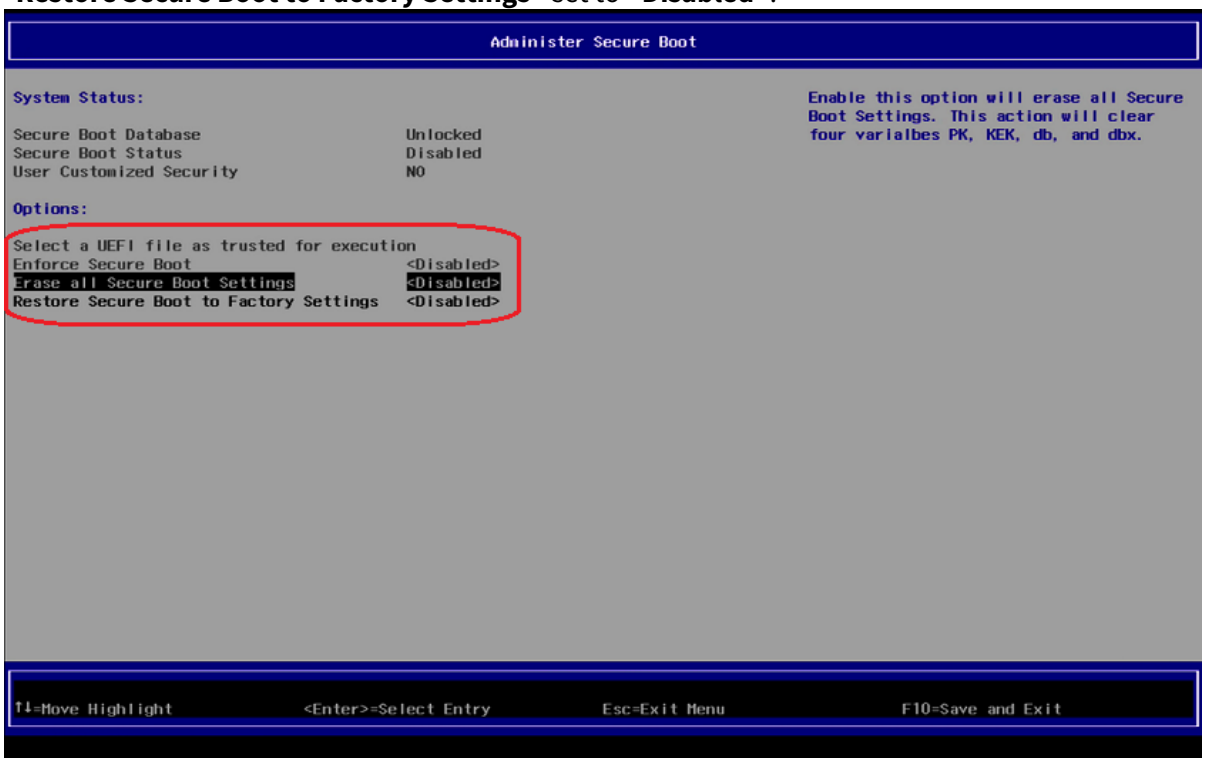
Activating the Secure Boot Feature

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

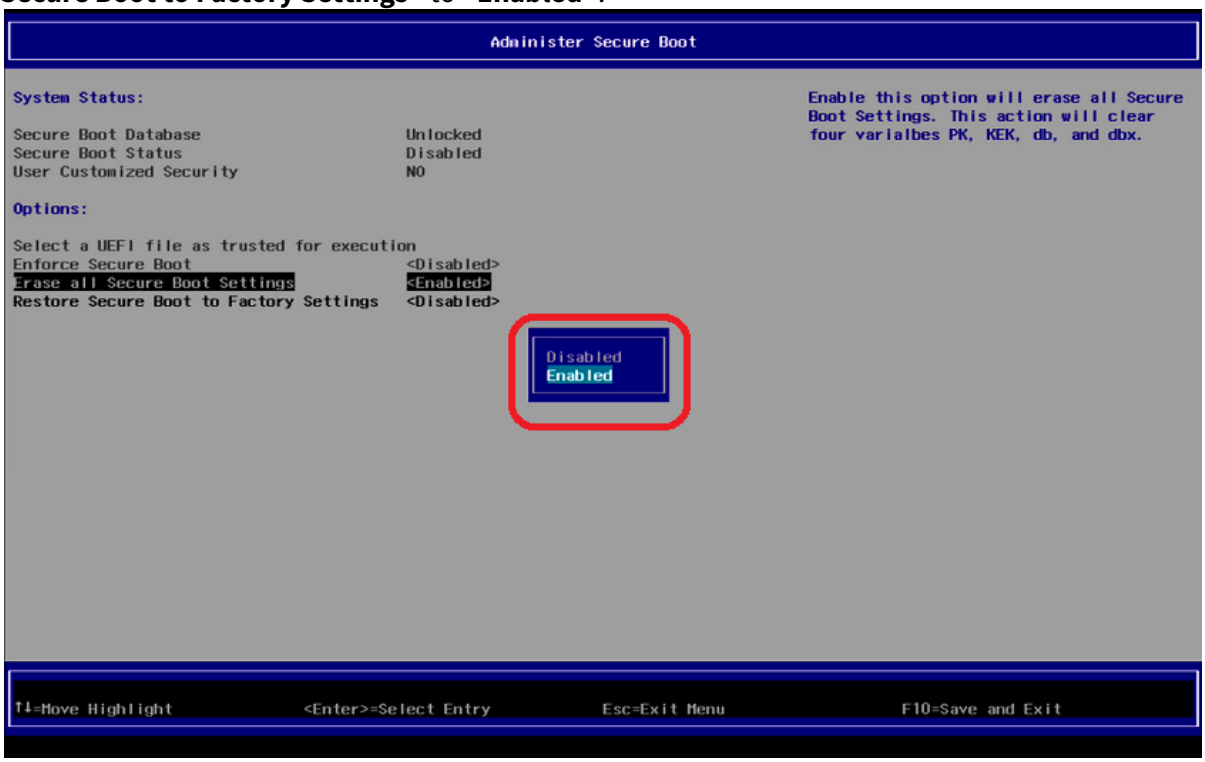
3. Using the arrow keys, move to the option **Secure Boot Option**, and press [ENTER]. This will open the the screen **Administer Secure Boot**.



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>**.

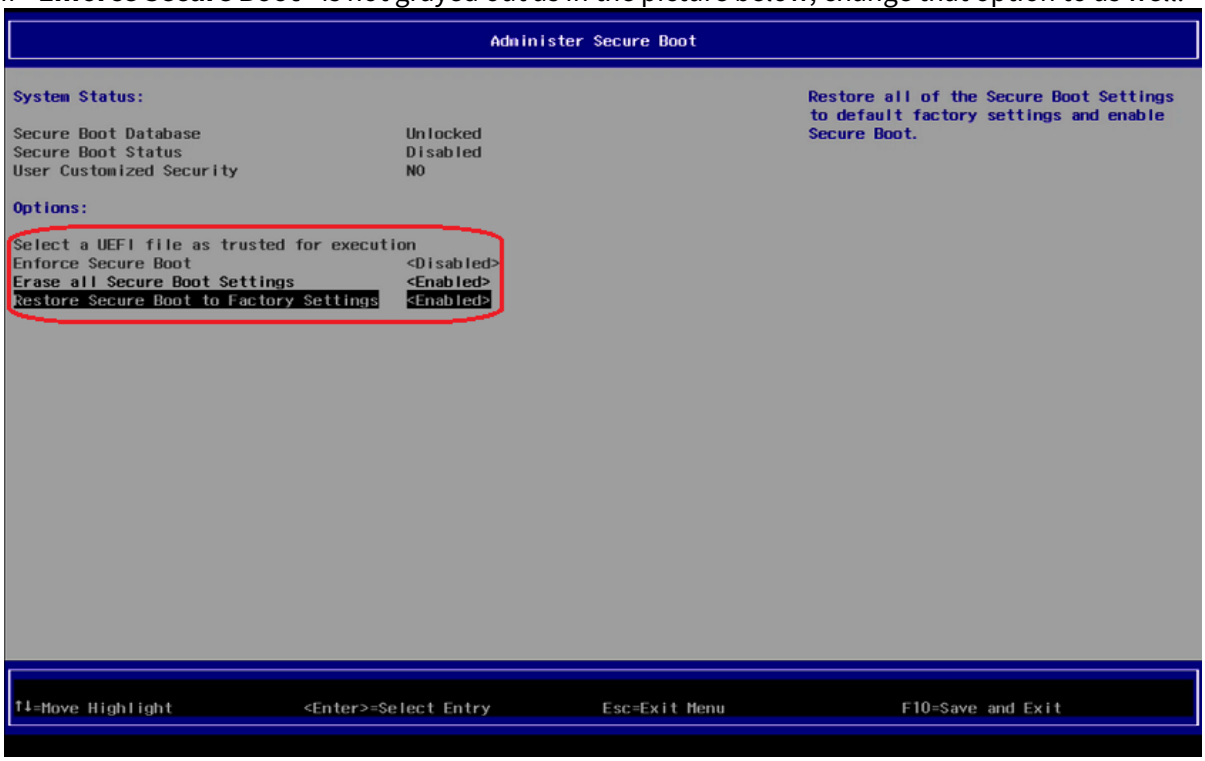


5. In the screen **Administer Secure Boot**, set "**Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.

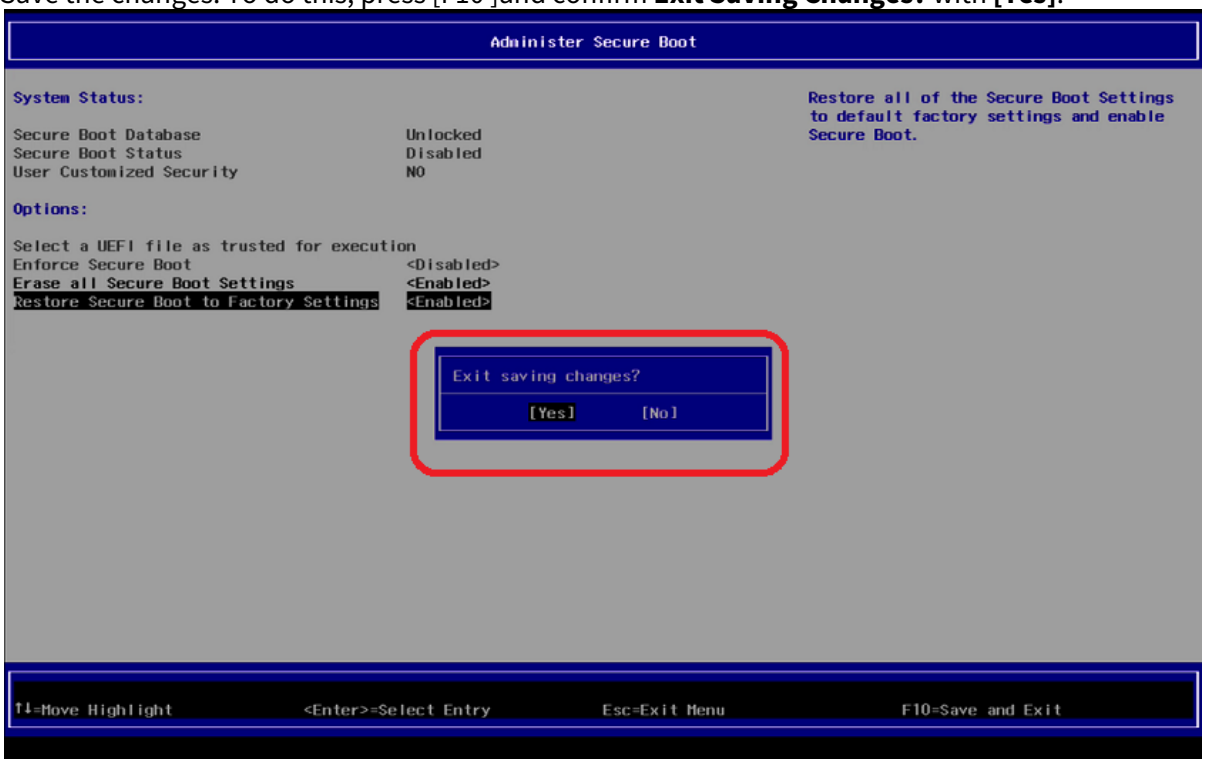


6. **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** are now set to **<Enabled>**.

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[39].

4.1.7 Enabling UEFI Secure Boot in UD7-LX 10

Prerequisites

- IGEL OS 10.04.100 or higher

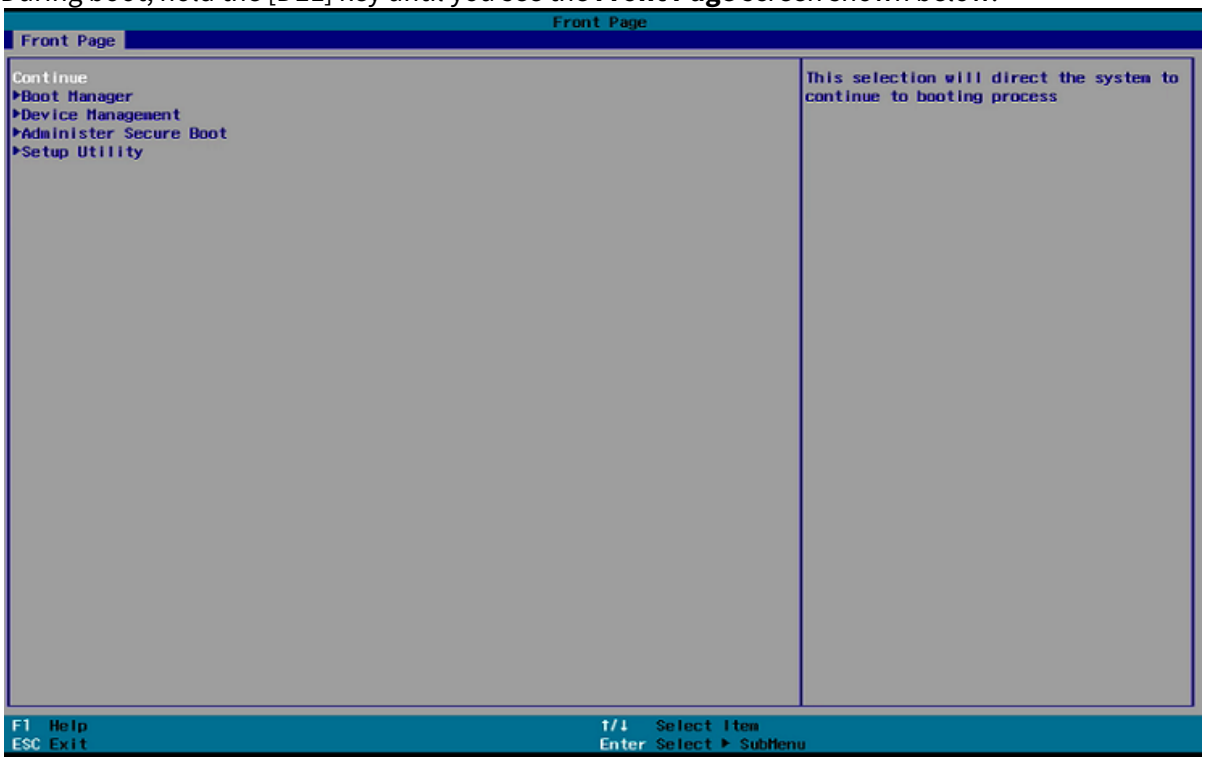
> The version of IGEL Linux can be found in the **About** window.

> 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.**

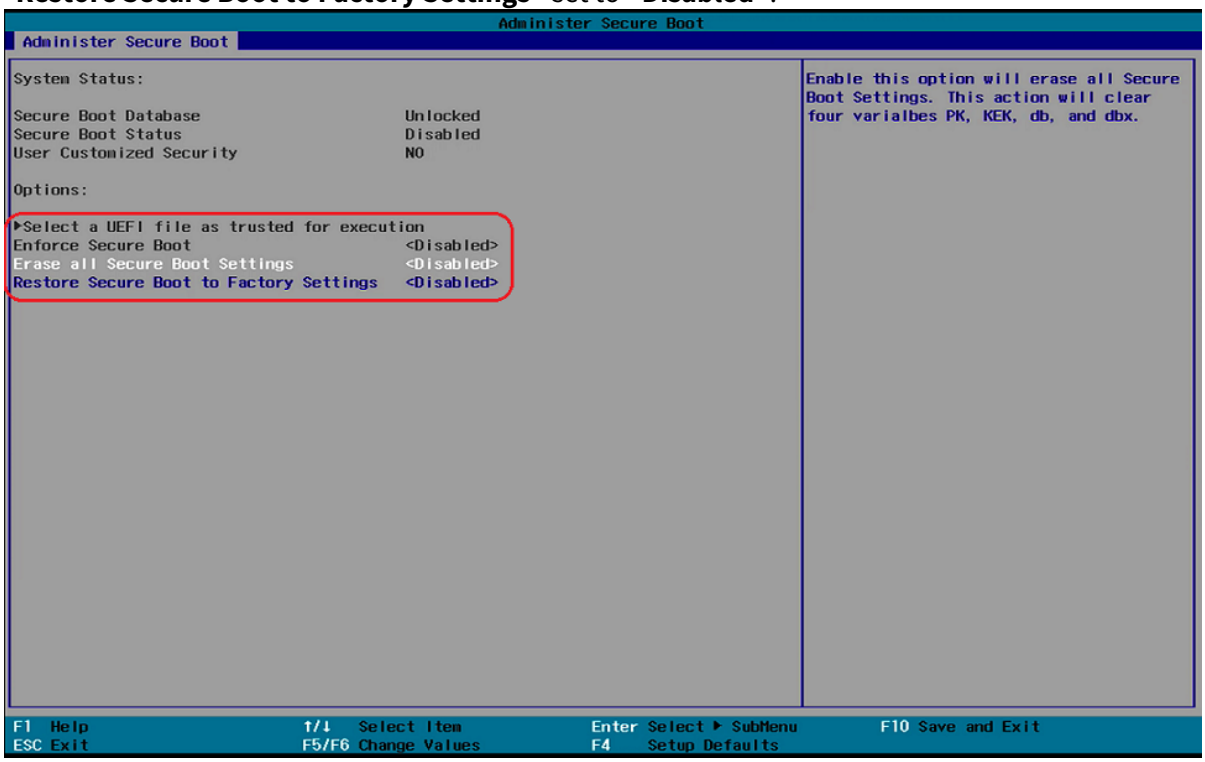
Activating the Secure Boot Feature

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



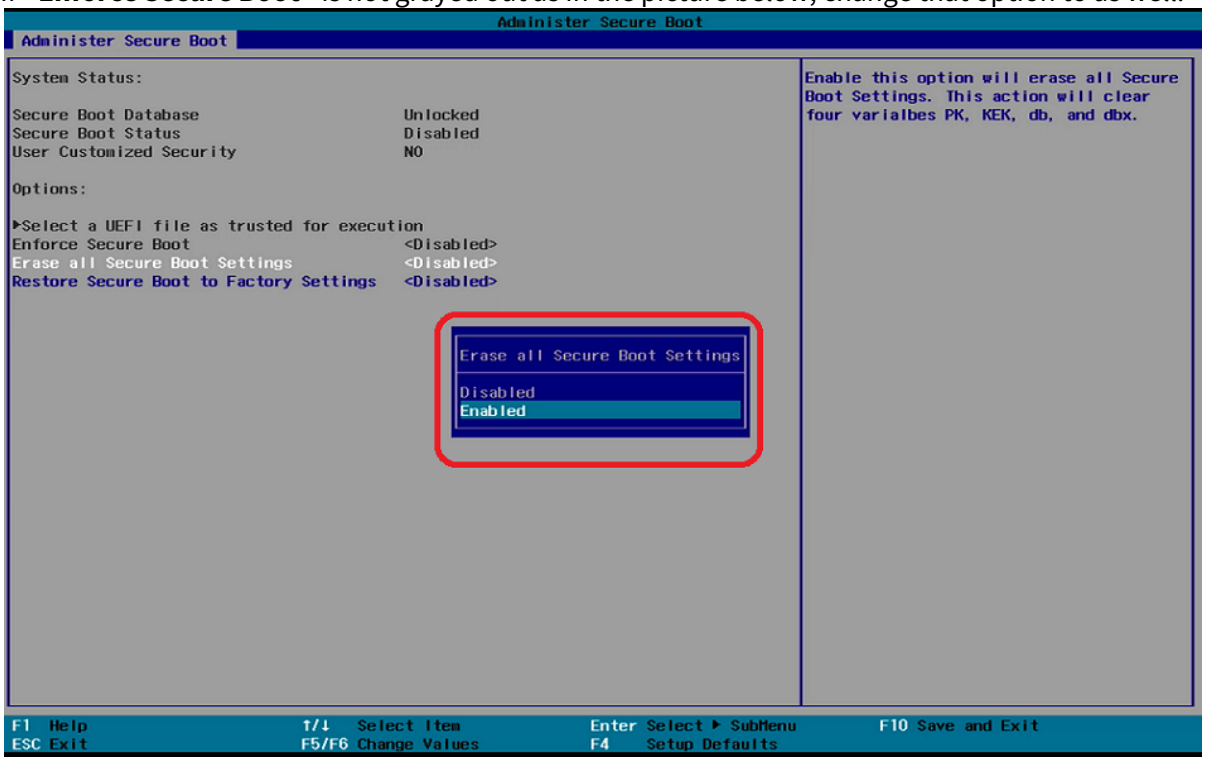
39 https://kb.igel.com/display/securitysafety/Veryfing+that+UEFI+Secure+Boot+is+enabled

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>**.

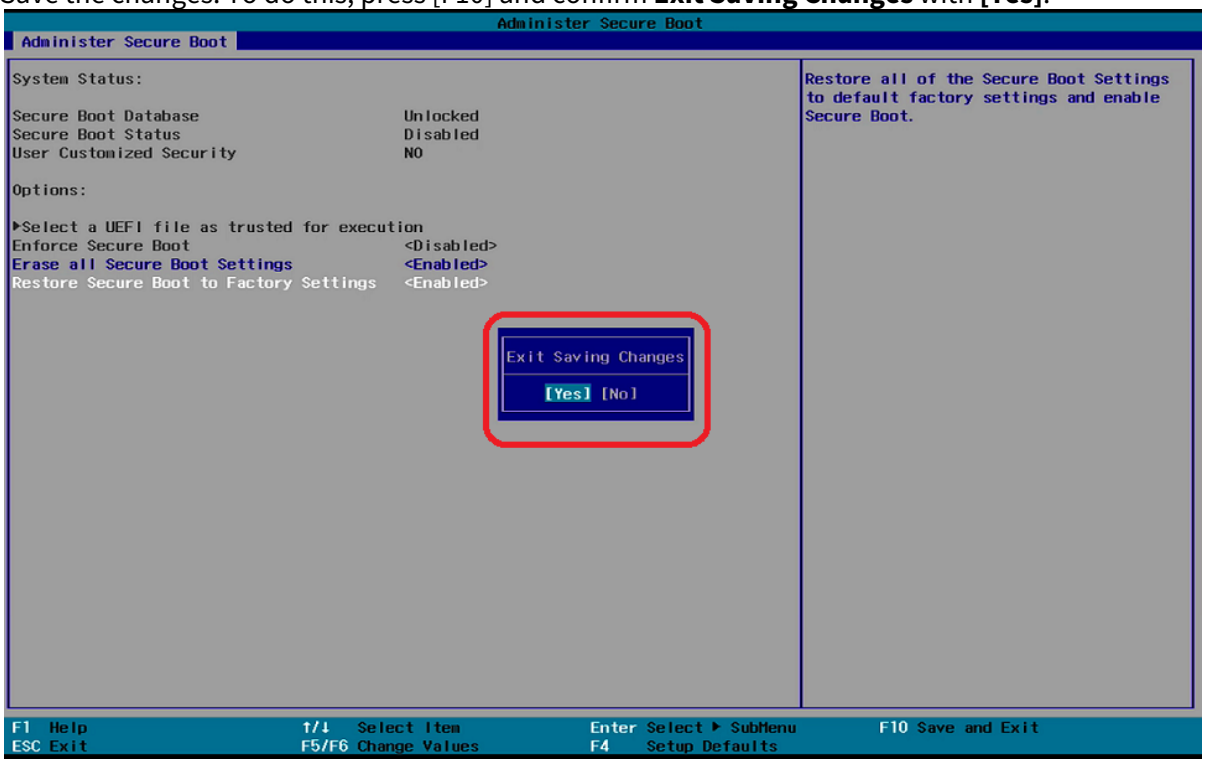


4. Change both **"Erase all Secure Boot Settings"** and **"Restore Secure Boot to Factory Settings"** to **<Enabled>**.

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[40].

4.1.8 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.

4.2 Microsoft Windows 10 IoT

- Enabling UEFI Secure Boot in UD3-W10 51 (see page 64)
- Enabling UEFI Secure Boot in UD6-W10 51 (see page 70)
- Enabling UEFI Secure Boot in UD7-W10 10 (see page 77)

4.2.1 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[41] corresponds to *3.A. 13-11202017* or newer.

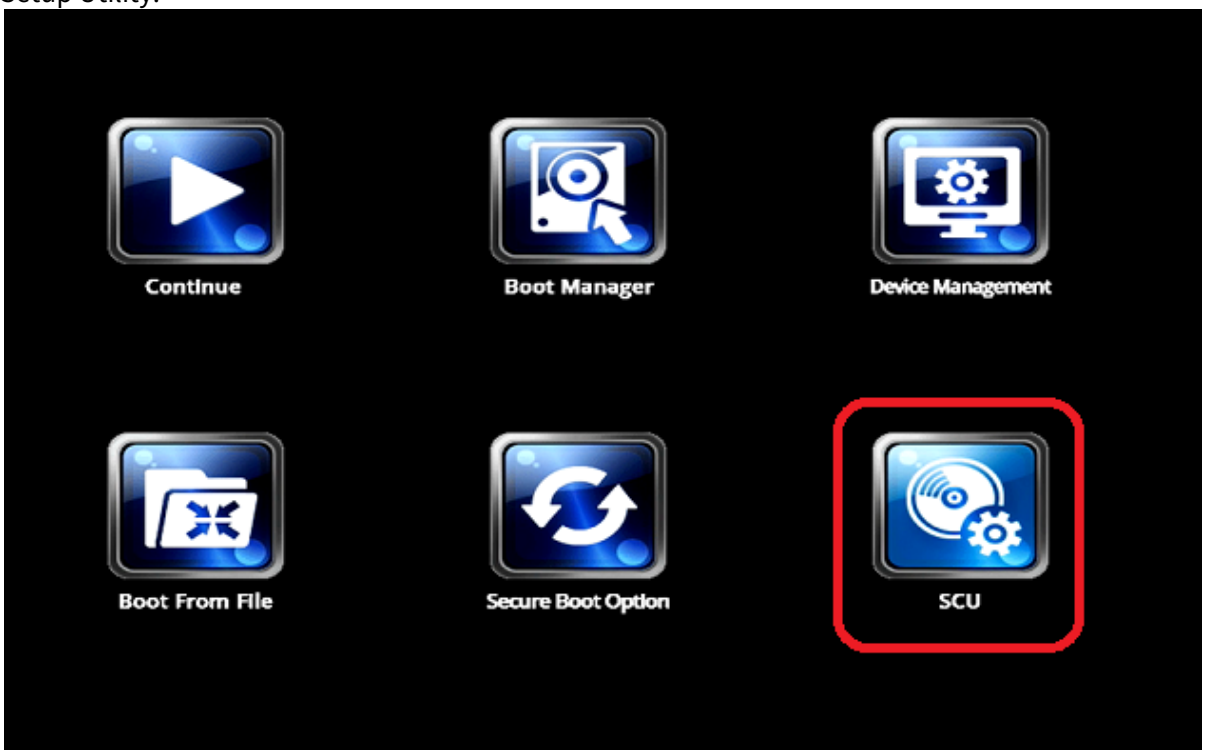
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Changing the Device's Boot Type to UEFI Boot

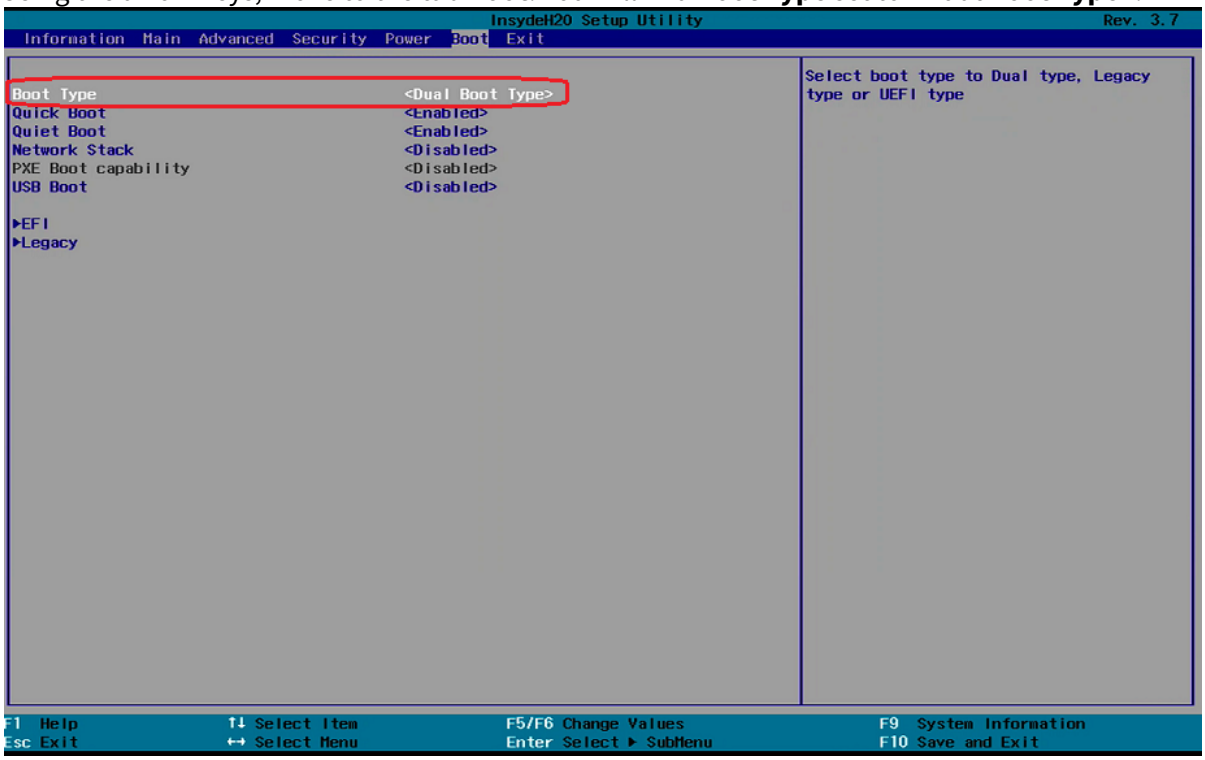
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.

40 https://kb.igel.com/display/securitysafety/Veryfing+that+UEFI+Secure+Boot+is+enabled
41 https://kb.igel.com/display/hardware/How+Can+I+Update+the+BIOS+Version

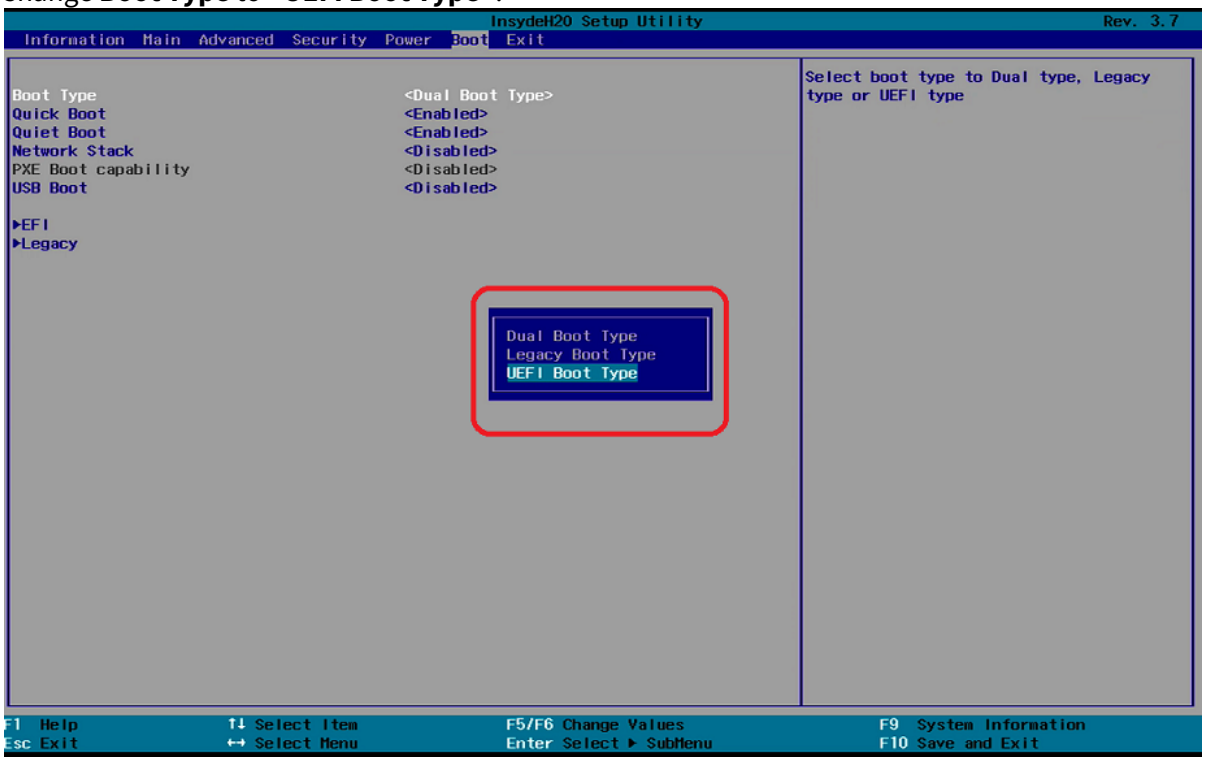
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



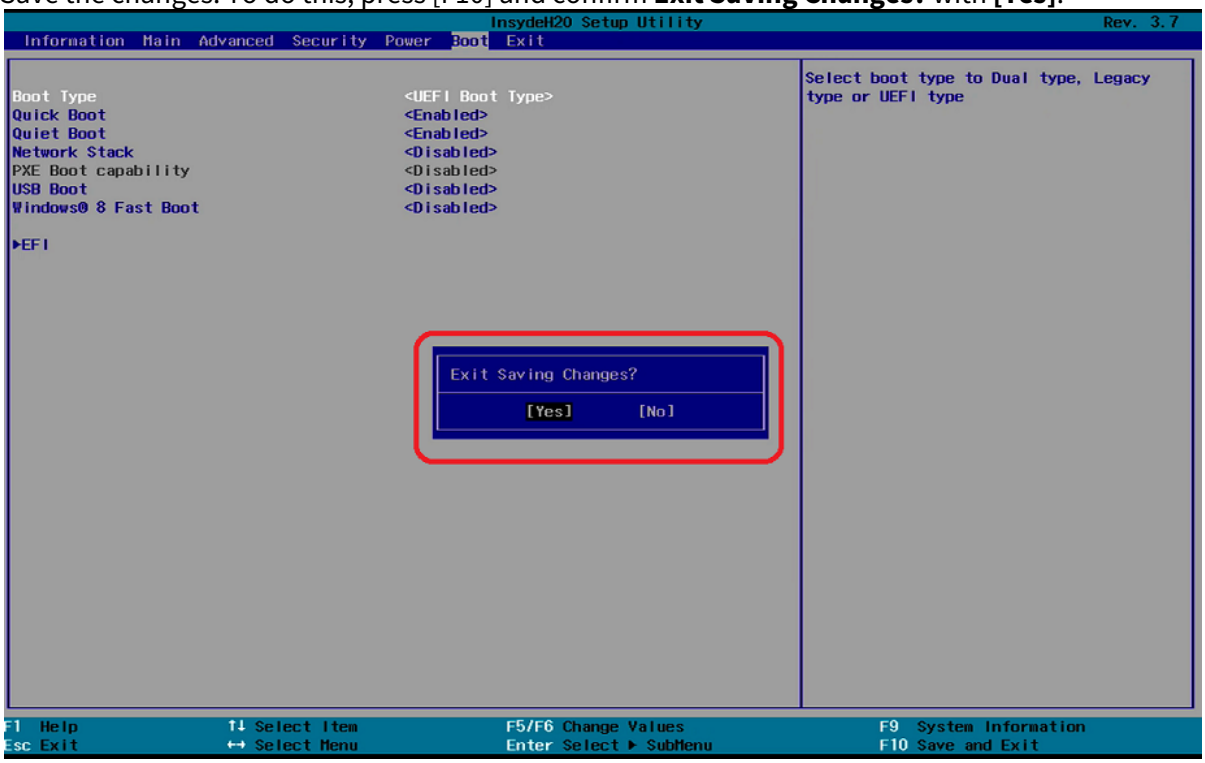
4. Using the arrow keys, move to the tab **Boot**. You will find **Boot Type** set to **<Dual Boot Type>**.



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



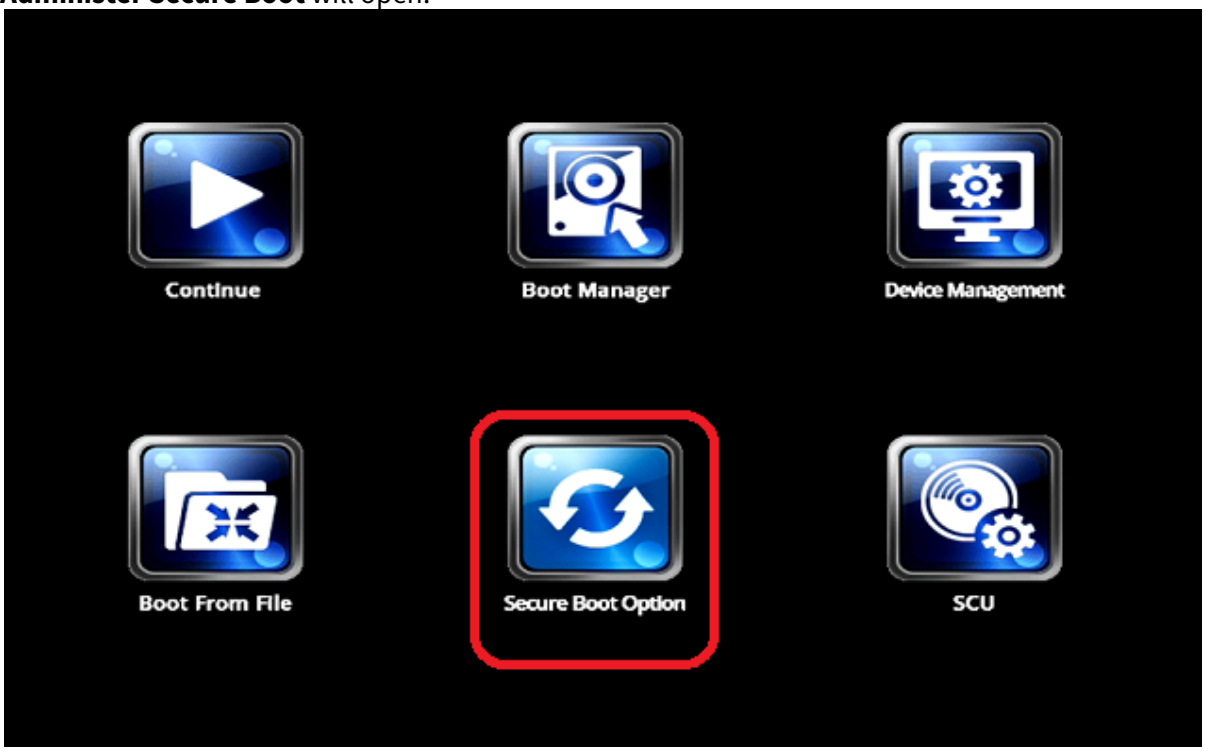
6. Save the changes. To do this, press [F10] and confirm **Exit Saving Changes?** with **[Yes]**.



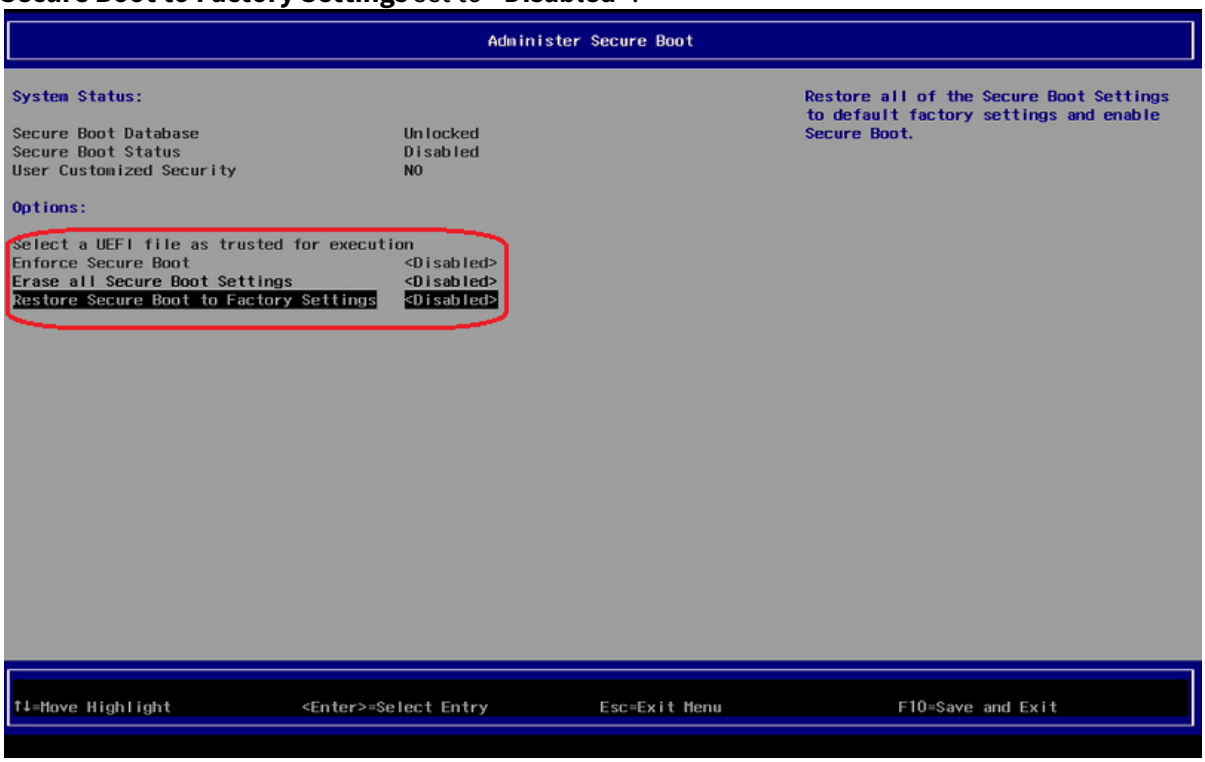
The changes will be saved and the device will be rebooted.

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.

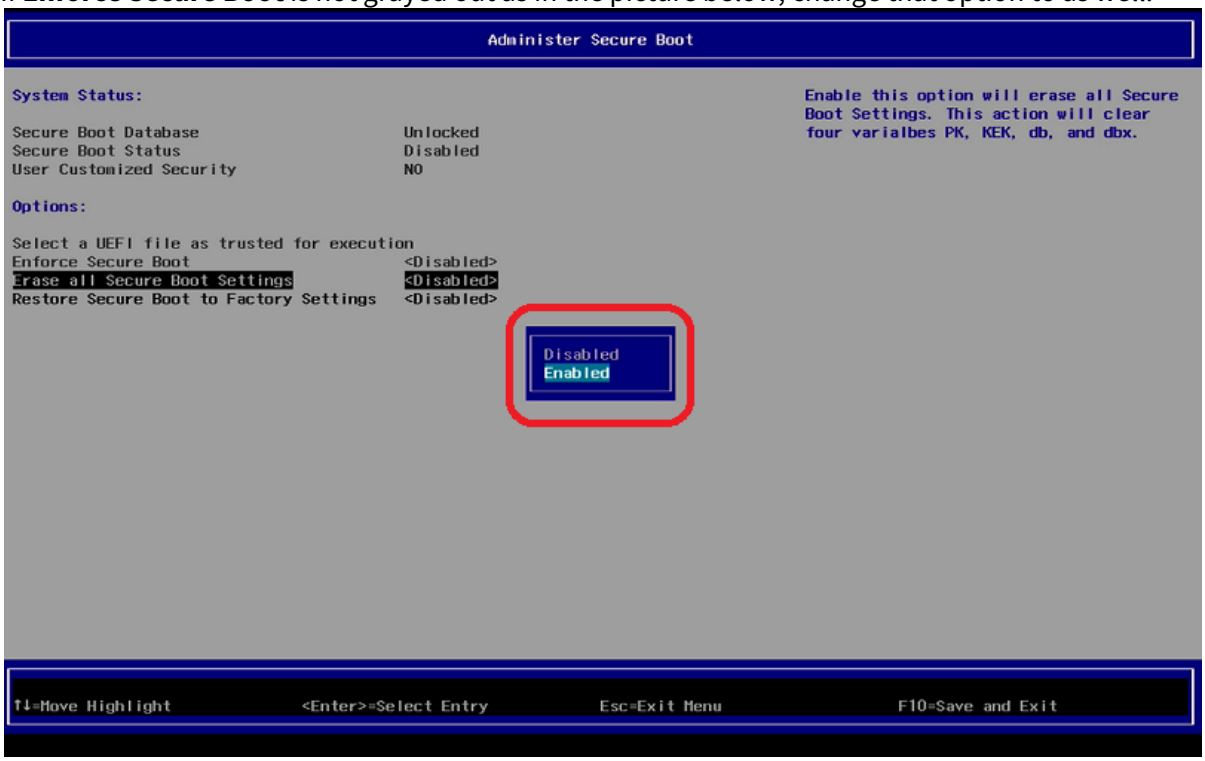


3. In the screen **Administer Secure Boot**, you will find **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** set to **<Disabled>**.

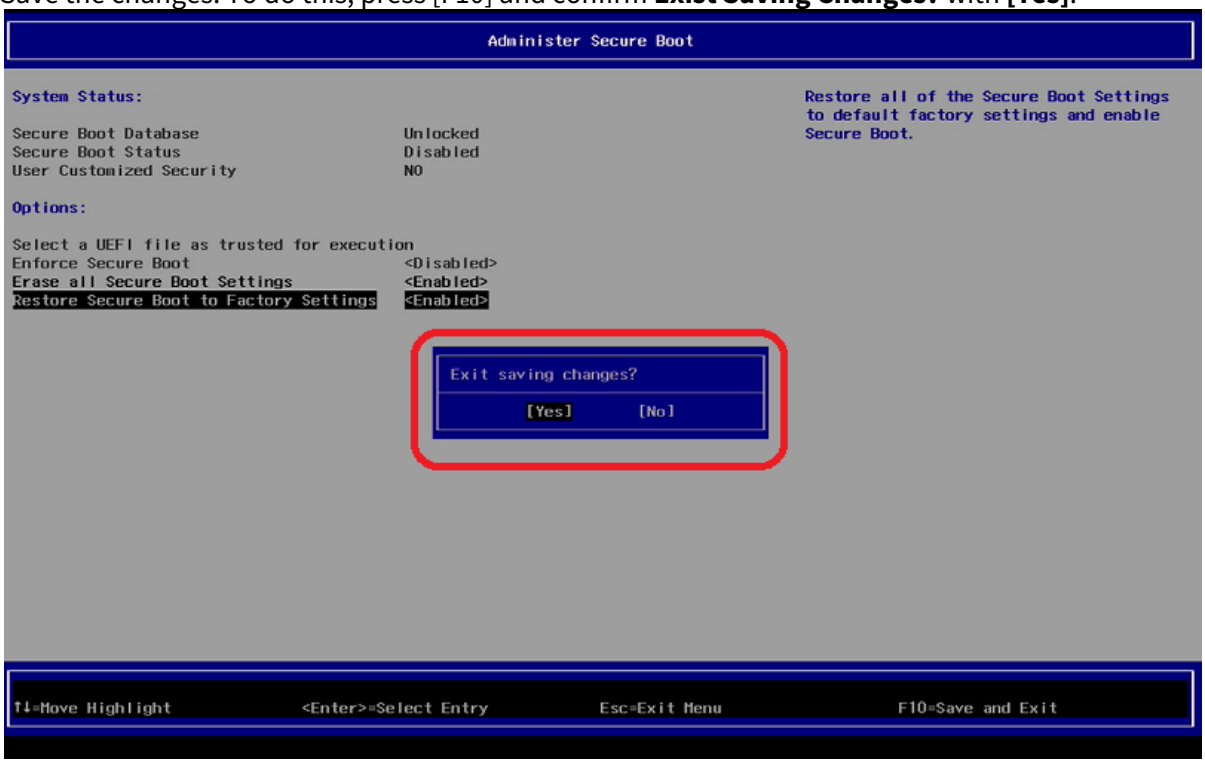


4. Change **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** to **<Enabled>**.

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[42].

4.2.2 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[43] corresponds to *3.9. 13-02202017* or newer.

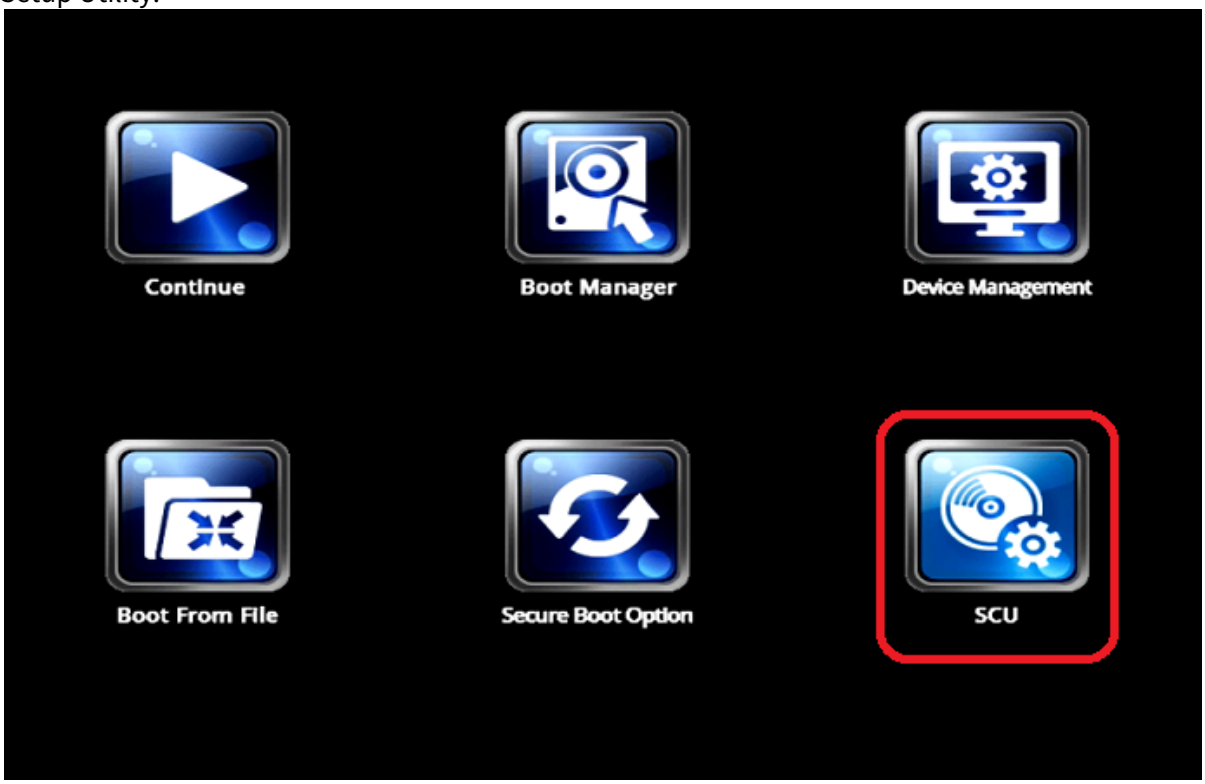
> **It is crucial to set a BIOS password to prevent users from disabling Secure Boot.**

Changing the Device's Boot Type to UEFI Boot

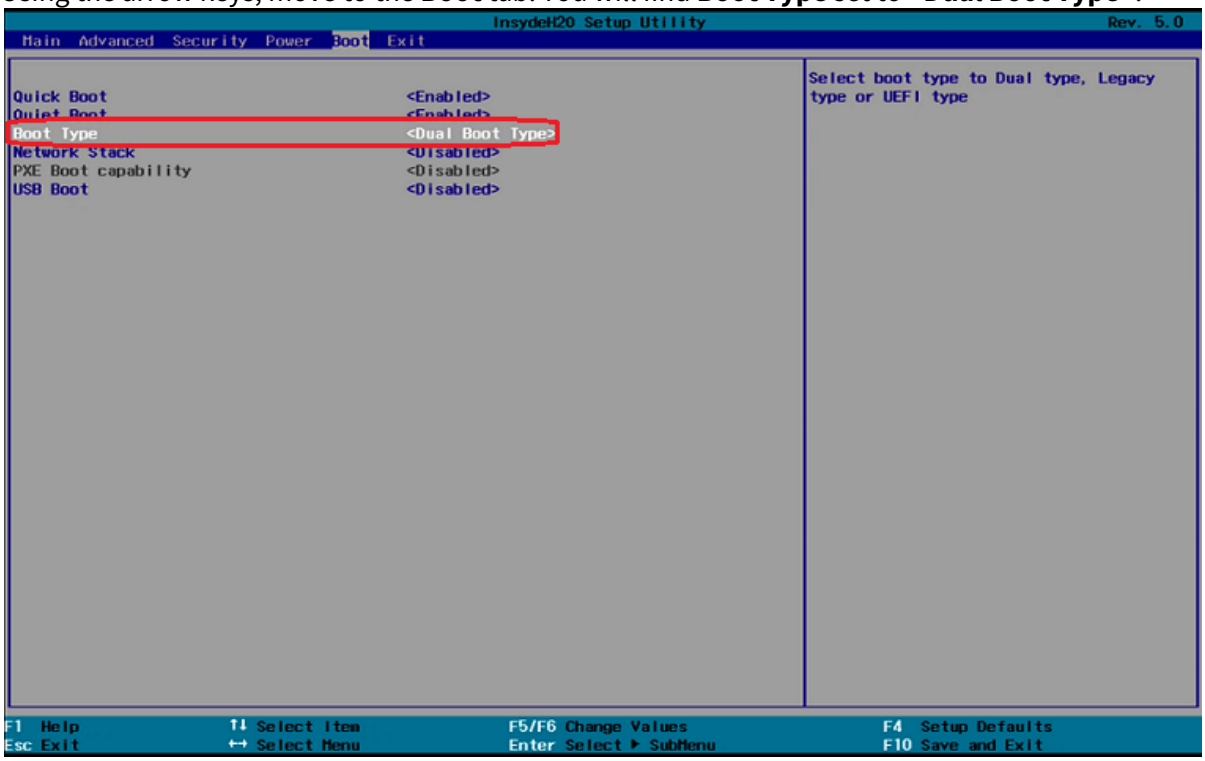
1. Turn on (or restart) the IGEL device.
2. During boot, hold the [DEL] key until you see the menu shown below.

42 https://kb.igel.com/display/securitysafety/Veryfing+that+UEFI+Secure+Boot+is+enabled
43 https://kb.igel.com/display/hardware/How+Can+I+Update+the+BIOS+Version

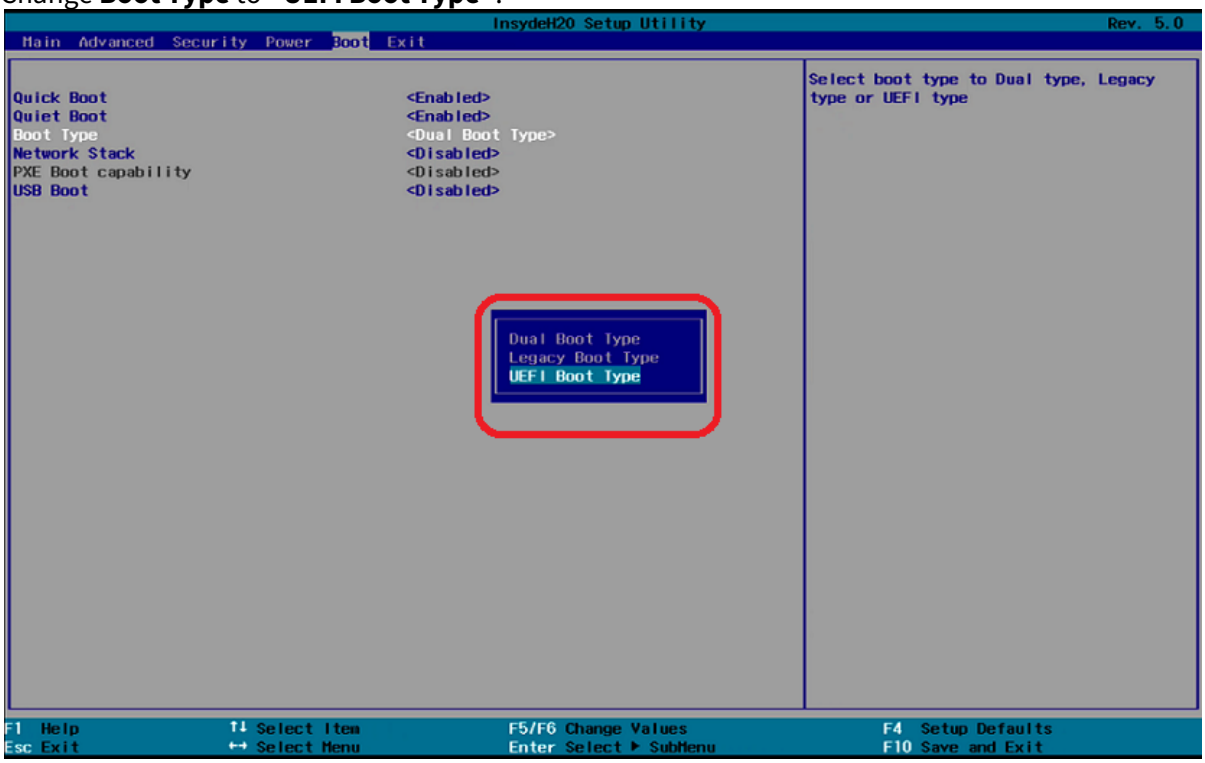
3. Using the arrow keys, navigate to the option **SCU** and press [ENTER]. This will open the InsydeH20 Setup Utility.



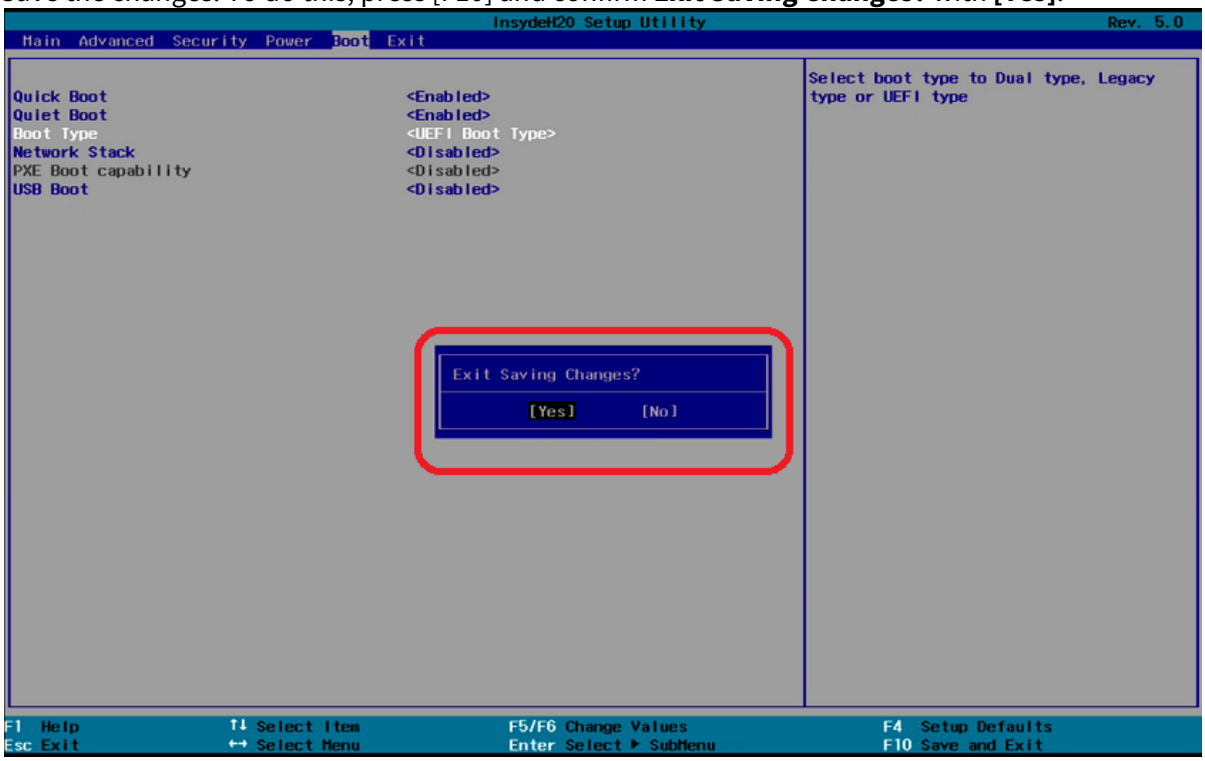
4. Using the arrow keys, move to the **Boot** tab. You will find **Boot Type** set to **<Dual Boot Type>**.



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



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

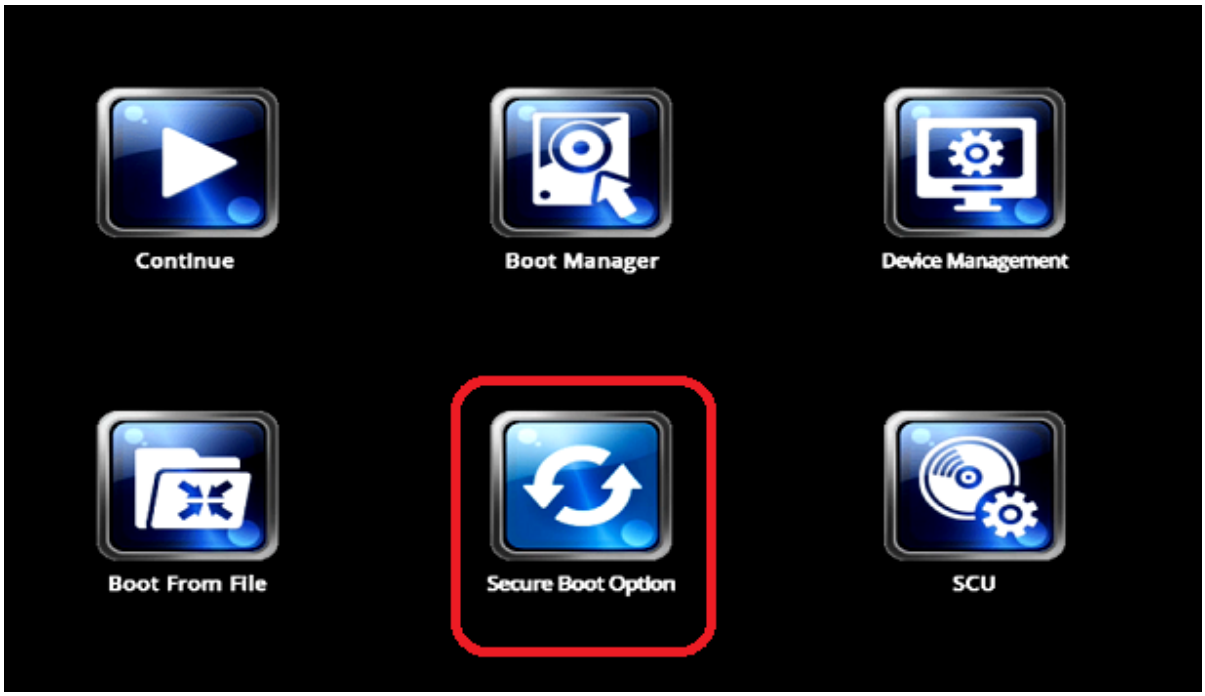


The changes will be saved and the device will be rebooted.

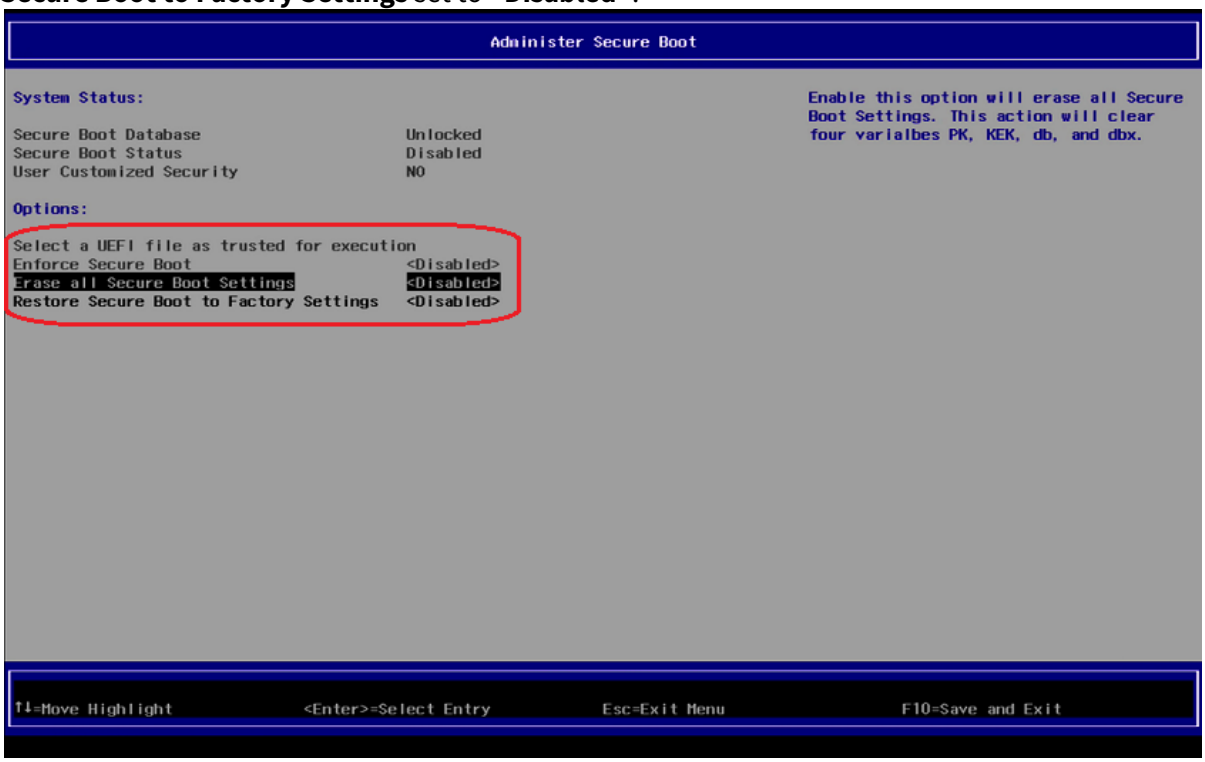
Activating the Secure Boot Feature

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

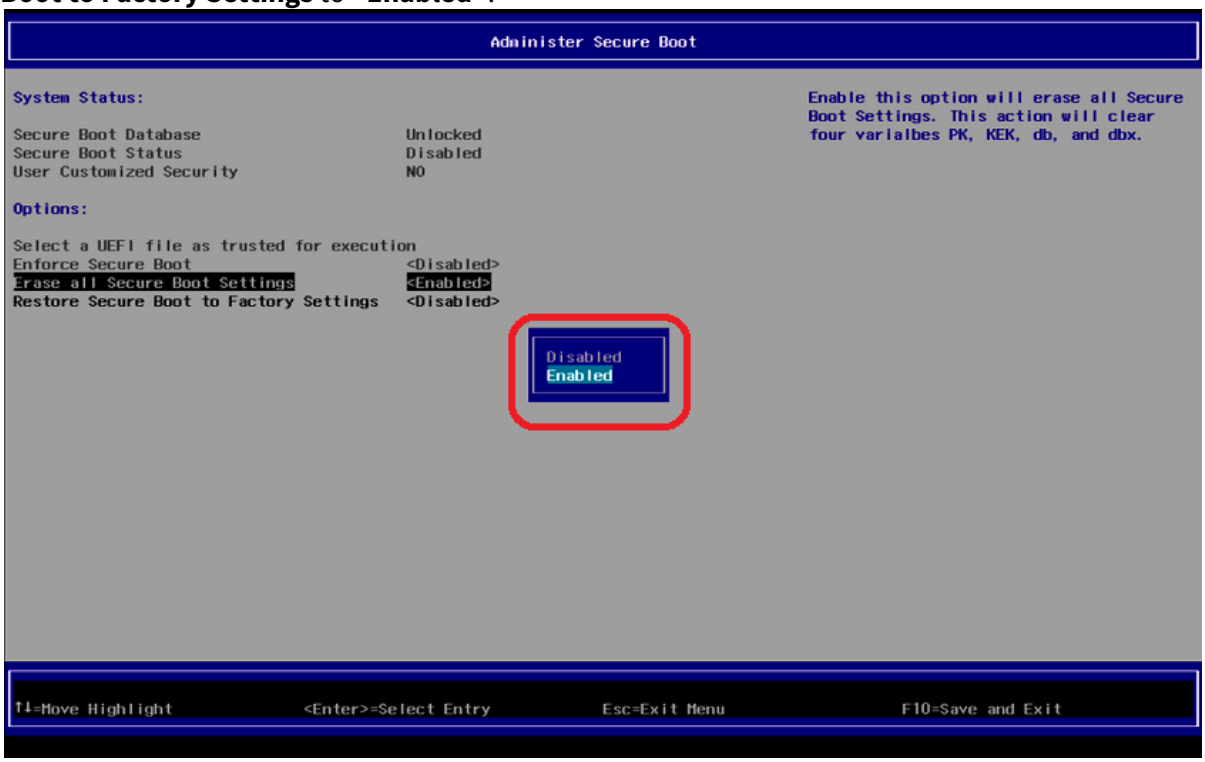
3. Using the arrow keys, move to the option **Secure Boot Option** and press [ENTER]. This will open the the screen **Administer Secure Boot**.



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>**.

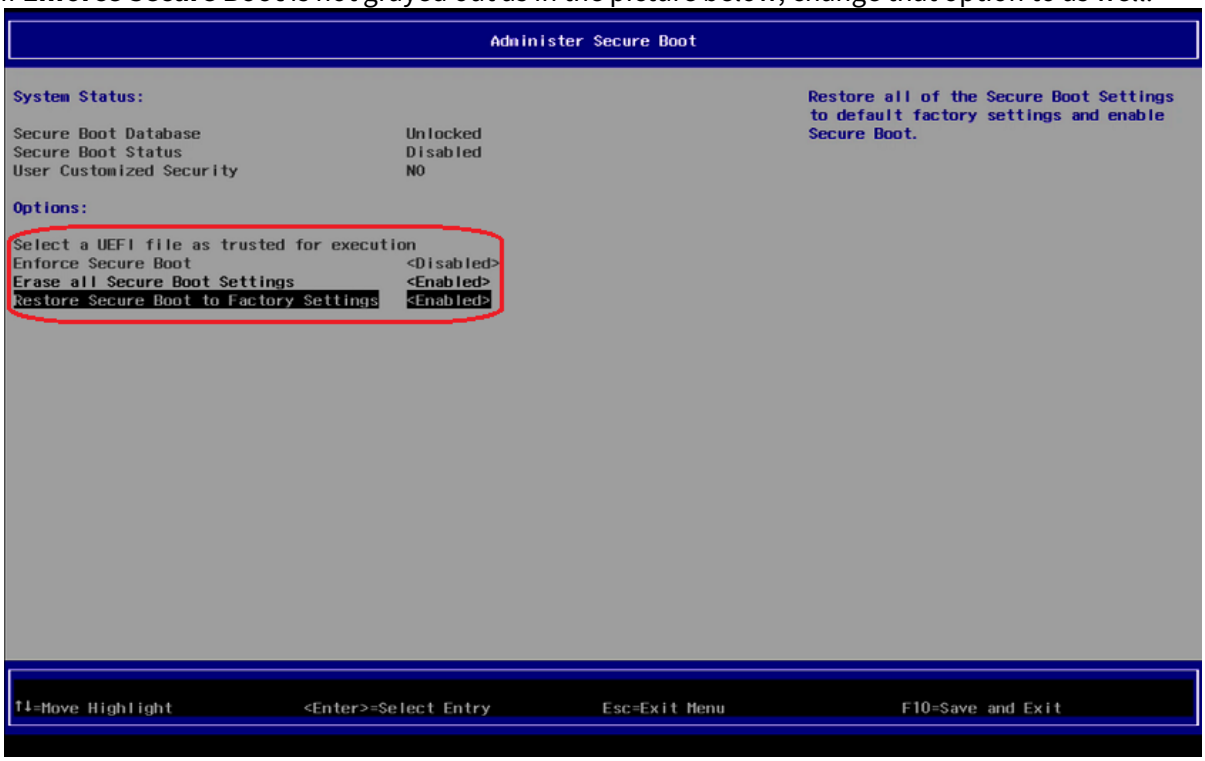


5. In the screen **Administer Secure Boot**, set **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** to **<Enabled>**.

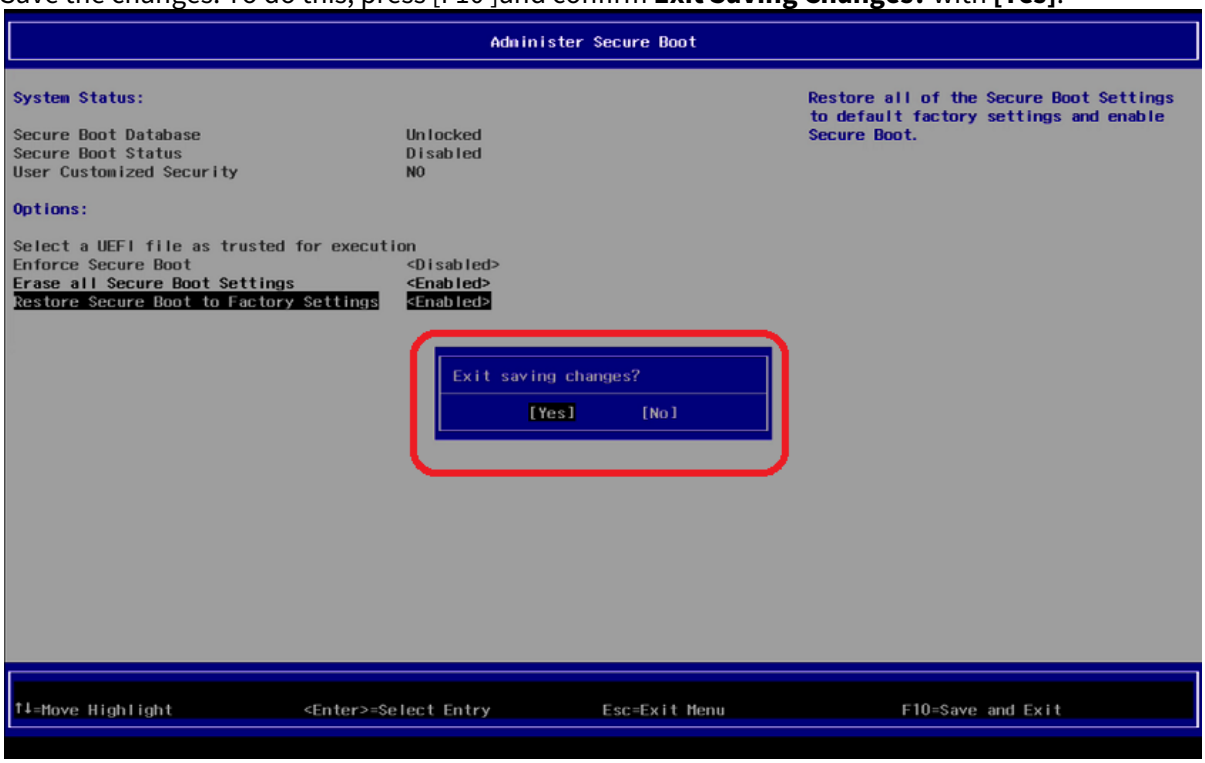


6. **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** are now set to **<Enabled>**.

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[44].

4.2.3 Enabling UEFI Secure Boot in UD7-W10 10

Prerequisites

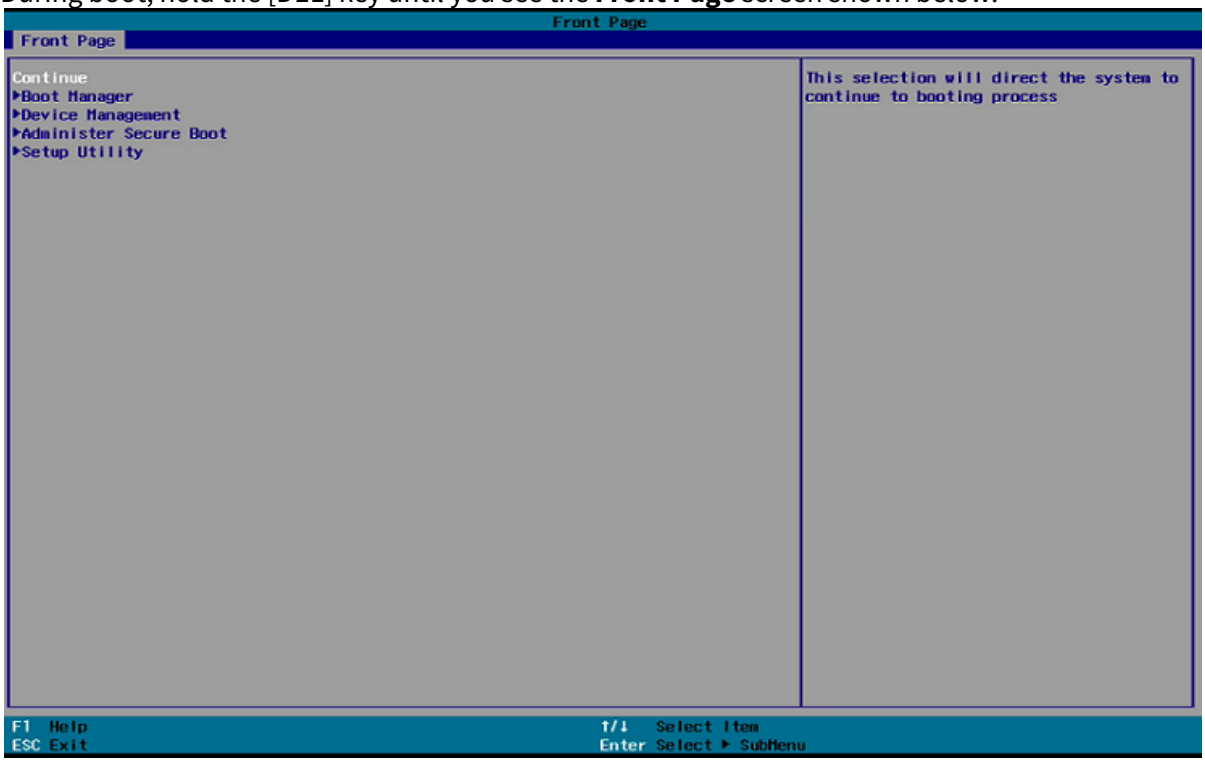
- Microsoft Windows IoT 4.03.100 or higher

> 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.**

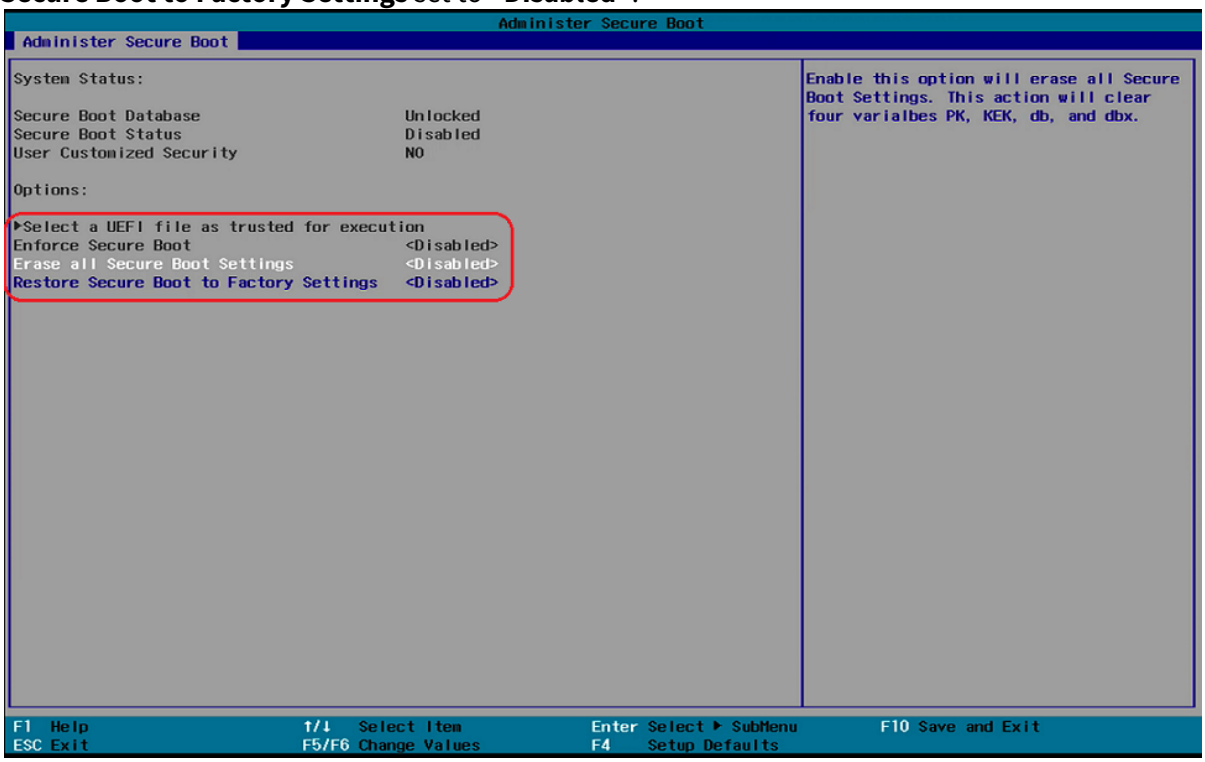
Activating the Secure Boot Feature

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



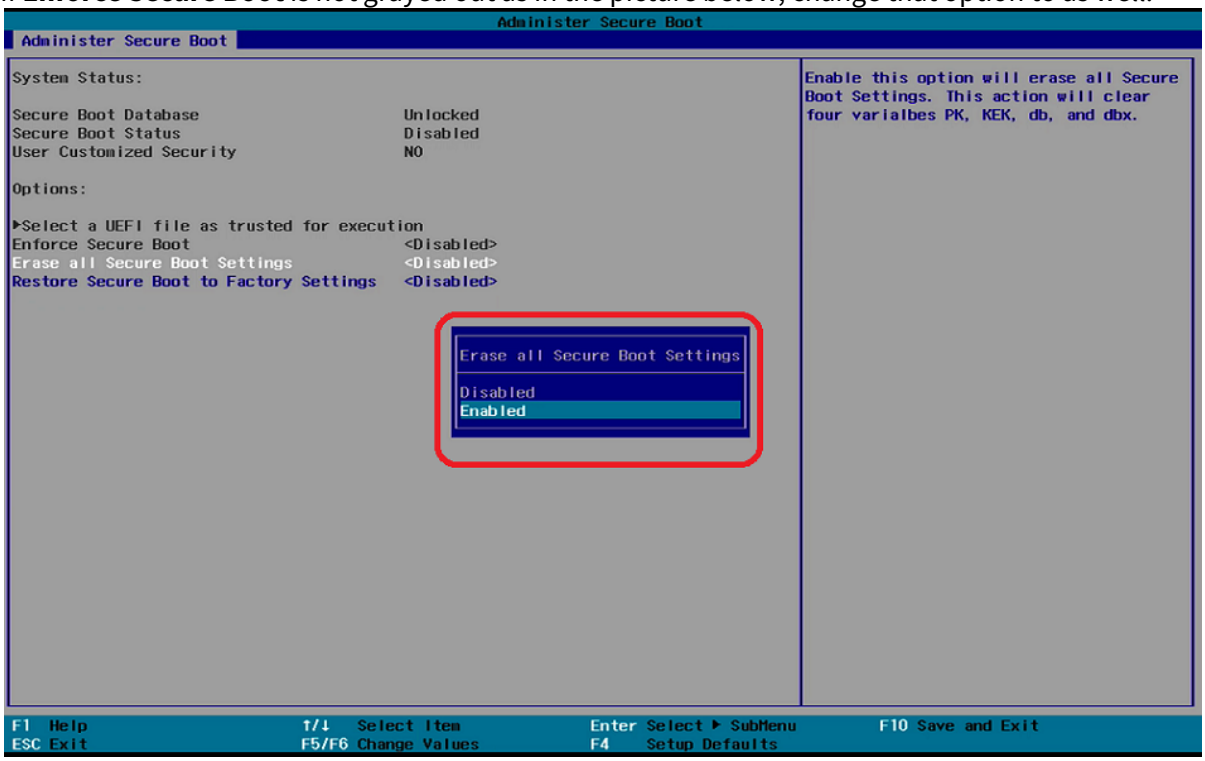
44 https://kb.igel.com/display/securitysafety/Veryfing+that+UEFI+Secure+Boot+is+enabled

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>**.

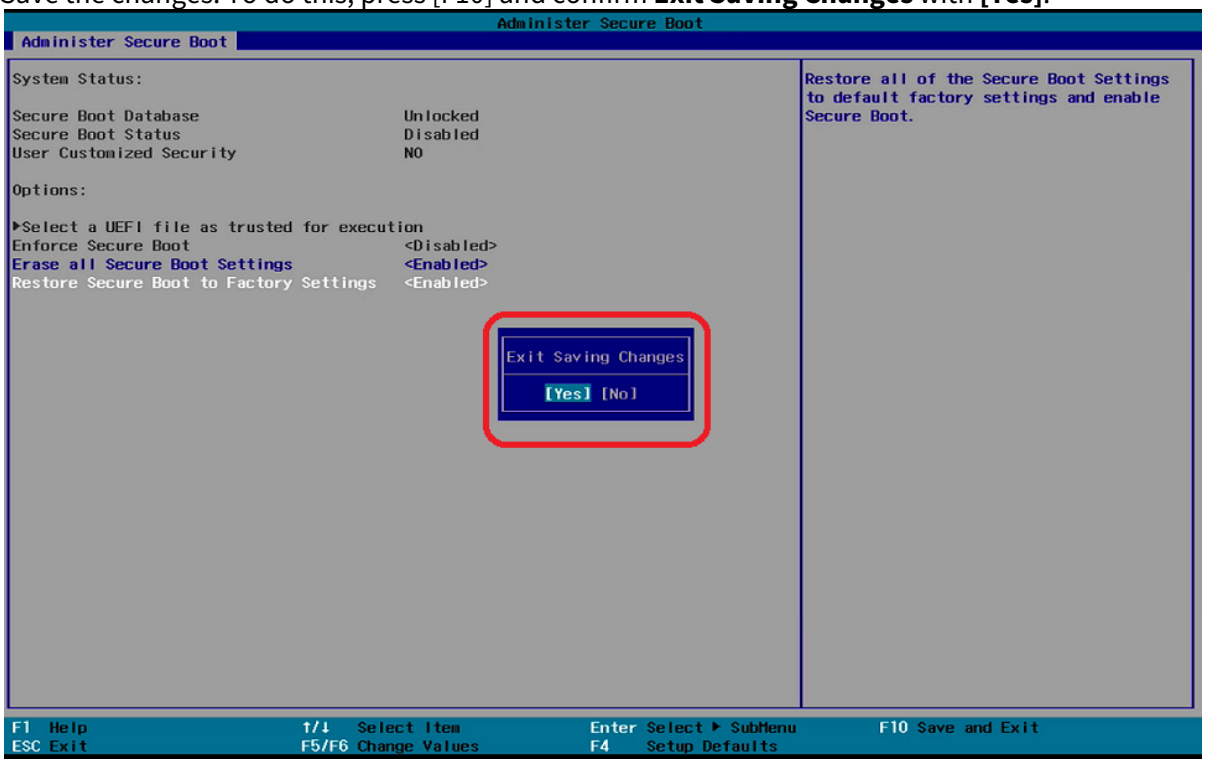


4. Change both **Erase all Secure Boot Settings** and **Restore Secure Boot to Factory Settings** to **<Enabled>**.

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[45].

4.3 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.

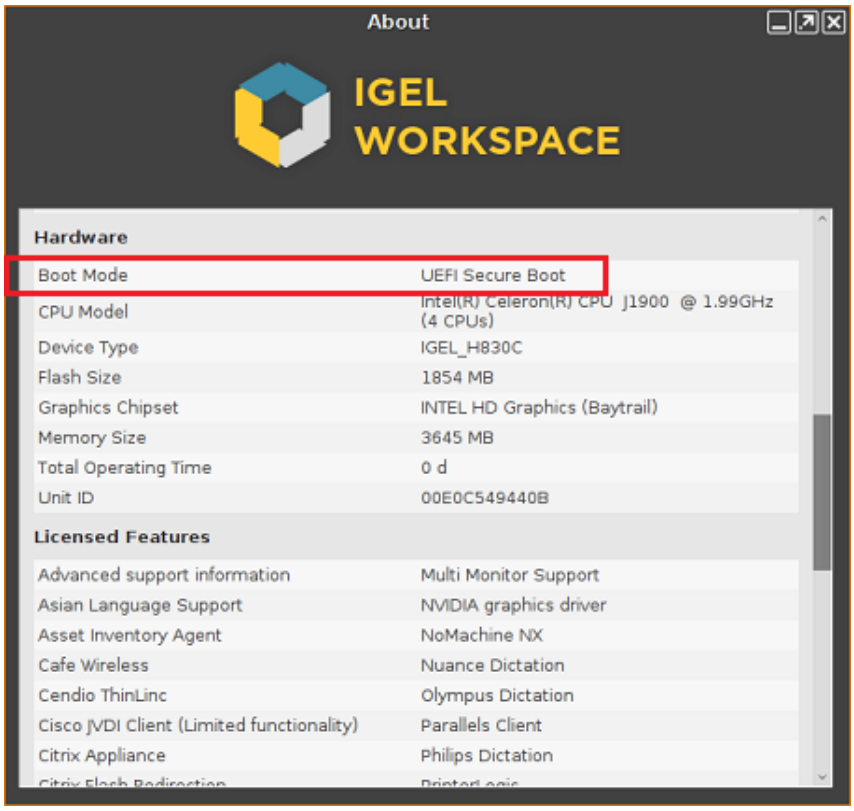
Check the following points to see whether UEFI Secure Boot has been properly enabled.

4.3.1 On IGEL OS 11.01.100 and Higher

- The boot splash contains a lock symbol.

45 https://kb.igel.com/display/securitysafety/Veryfing+that+UEFI+Secure+Boot+is+enabled

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



4.3.2 On IGEL OS 10.04.100 - 10.05.500

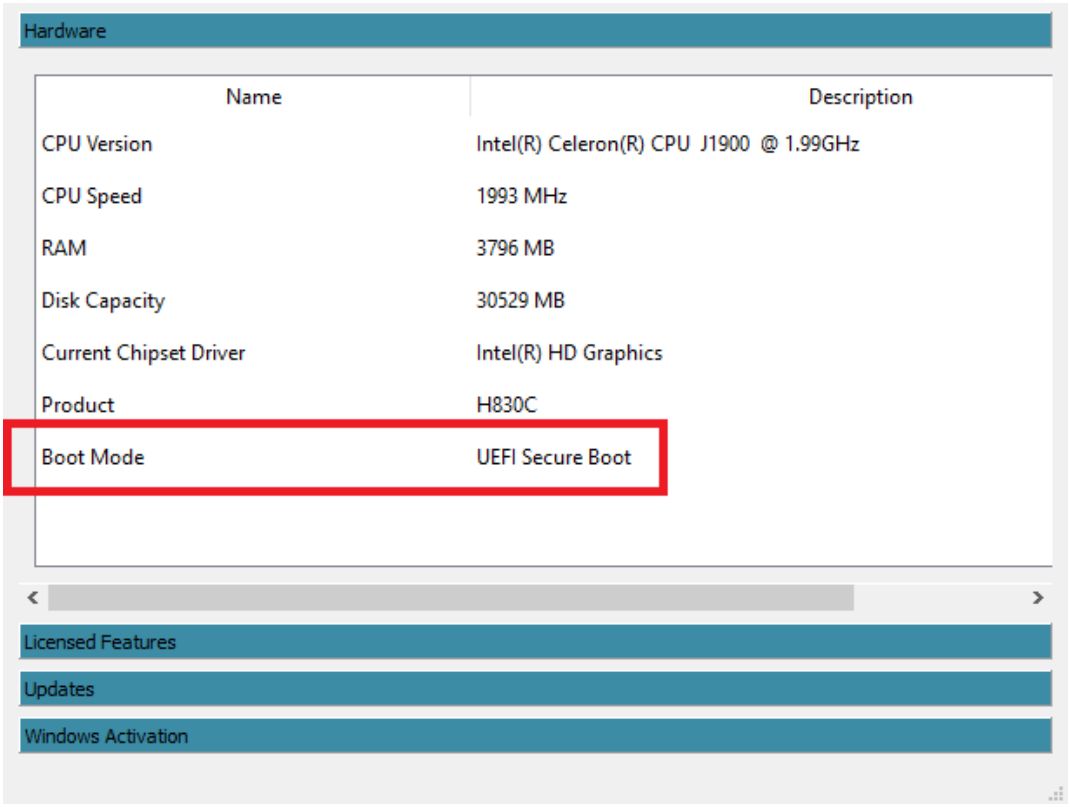
- The boot splash contains a lock symbol.

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

4.3.3 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

5 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/.

5.1 IGEL Devices with the Integrated AMD Secure Processor

- UD3 Model M350C[46]
- UD7 Model H860C[47]
- UD7 Model H850C(see page 84)

5.2 UD7 Model H850C

As from December 2019, IGEL UD7 model H850C is equipped with the AMD Secure Processor(see page 84).

> 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.

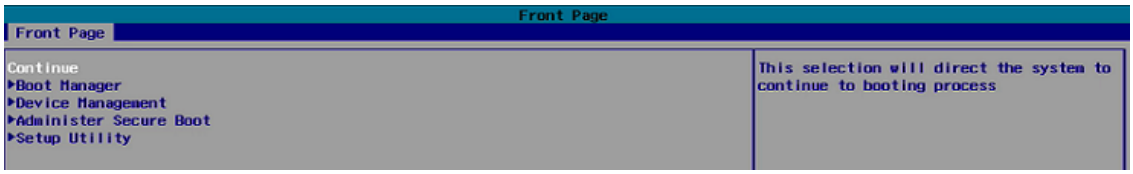
> The AMD Secure Processor technology increases the system boot time between 3 and 4.5 seconds.

5.2.1 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.

46 https://kb.igel.com/display/hardware/Technical+Specification%2C+UD3+model+M350C
47 https://kb.igel.com/display/hardware/Technical+Specification%2C+UD7+model+H860C



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:

6 AMD Memory Guard

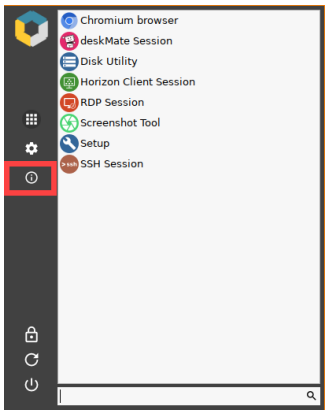
With AMD Memory Guard, IGEL enhances the security capabilities of the UD3 model M350C[48] and UD7 model H860C[49].

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 84) integrated in the IGEL device.

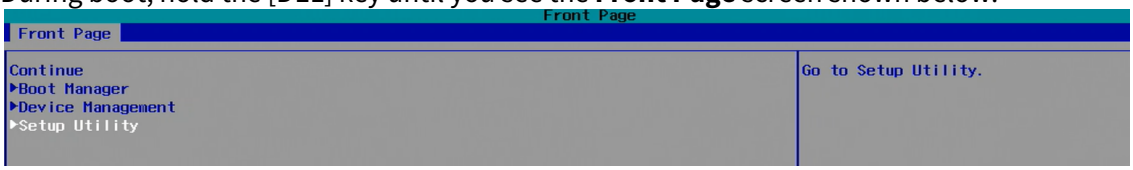
For more information about AMD Memory Guard, see https://www.amd.com/system/files/documents/amd-memory-guard-white-paper.pdf.

6.1 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.



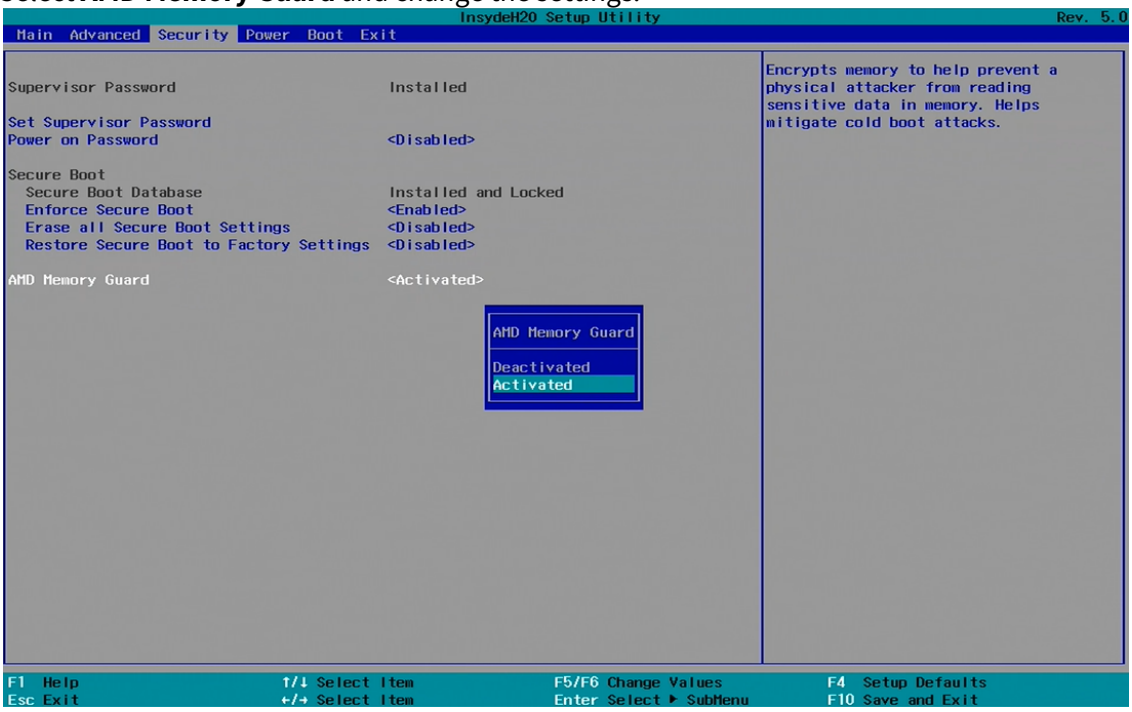
- AMD Memory Guard can be deactivated in BIOS under **Setup Utility > Security**.
  How to deactivate AMD Memory Guard
  a. Turn on (or restart) your device.
  b. During boot, hold the [DEL] key until you see the **Front Page** screen shown below.



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

48 https://kb.igel.com/display/hardware/Technical+Specification%2C+UD3+model+M350C
49 https://kb.igel.com/display/hardware/Technical+Specification%2C+UD7+model+H860C

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.

7 Security FAQs

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

7.1.1 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.

8 BSI Grundschutz

This document is available in German only.

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

This document is available in German only.

8.1.1 Über dieses Dokument

This document is available in German only.

8.1.2 Grundsätzliche Vorgaben zur Administration

This document is available in German only.

8.1.3 Fernwartung

This document is available in German only.

8.1.4 Zugriffskontrolle

This document is available in German only.

8.1.5 Absicherung des Bootvorgangs

This document is available in German only.

8.1.6 Schutz bei Diebstahl oder Defekt

This document is available in German only.

8.1.7 Schutz vor Manipulation

This document is available in German only.

8.1.8 Einschränken der Benutzerumgebung

This document is available in German only.

8.1.9 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

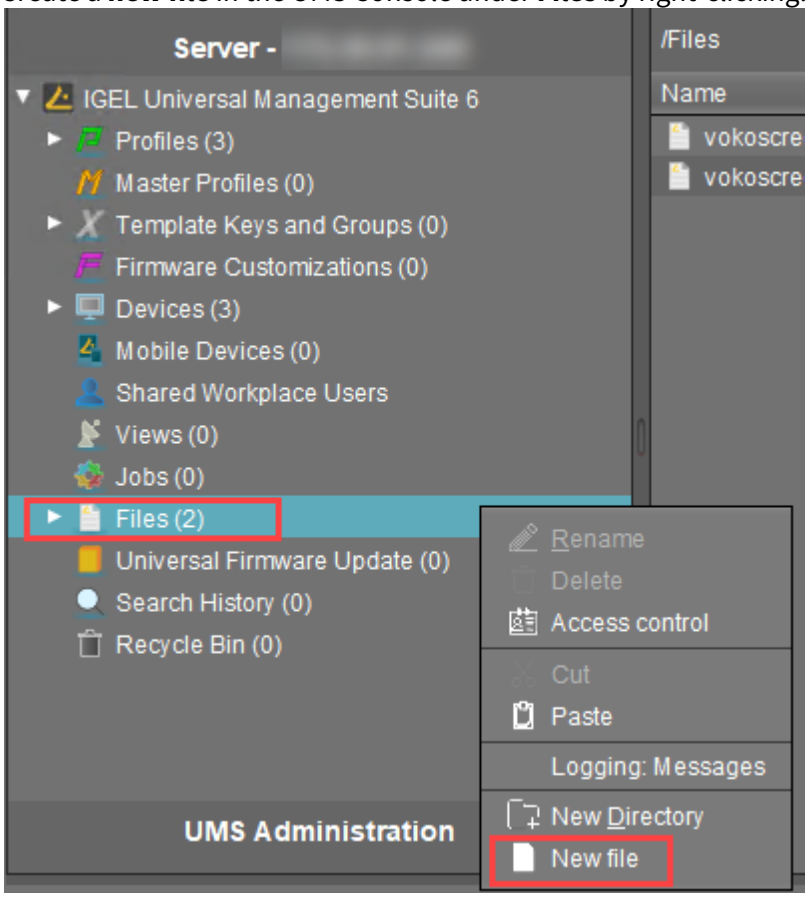
Use a log collector and analyzer, which allows the archiving and analysis of logs according to many aspects, such as Graylog, Splunk or the Elastic-Logstash-Kibana-Stack (ELK). Their evaluation function must be able to differentiate according to the types of data required for logging (for example, filtering 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

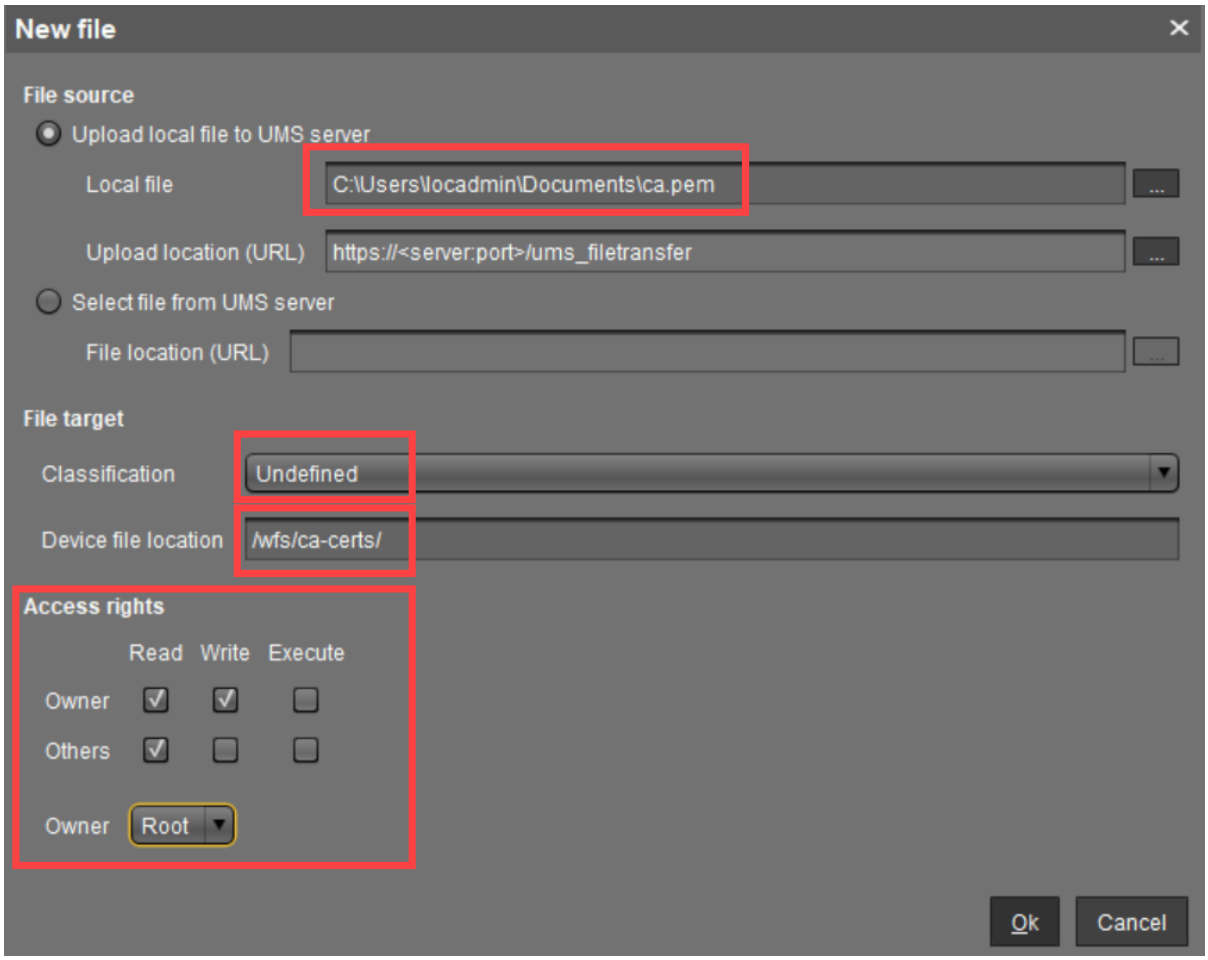
If the X.509 certificate of your log collector is not signed by a CA known to IGEL OS, install the CA root certificate of the signer as follows:

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**.

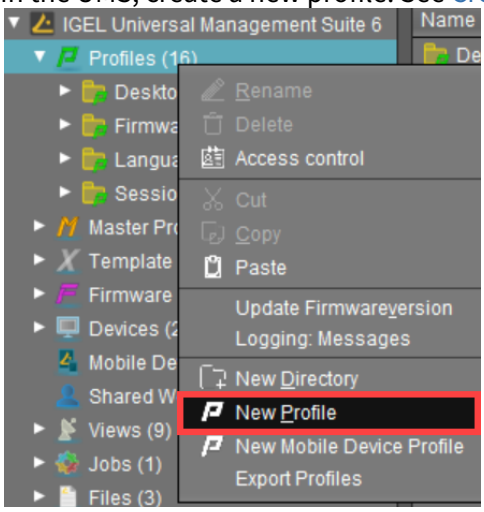


6. Click **Ok**.
7. Assign the file object to the desired devices.

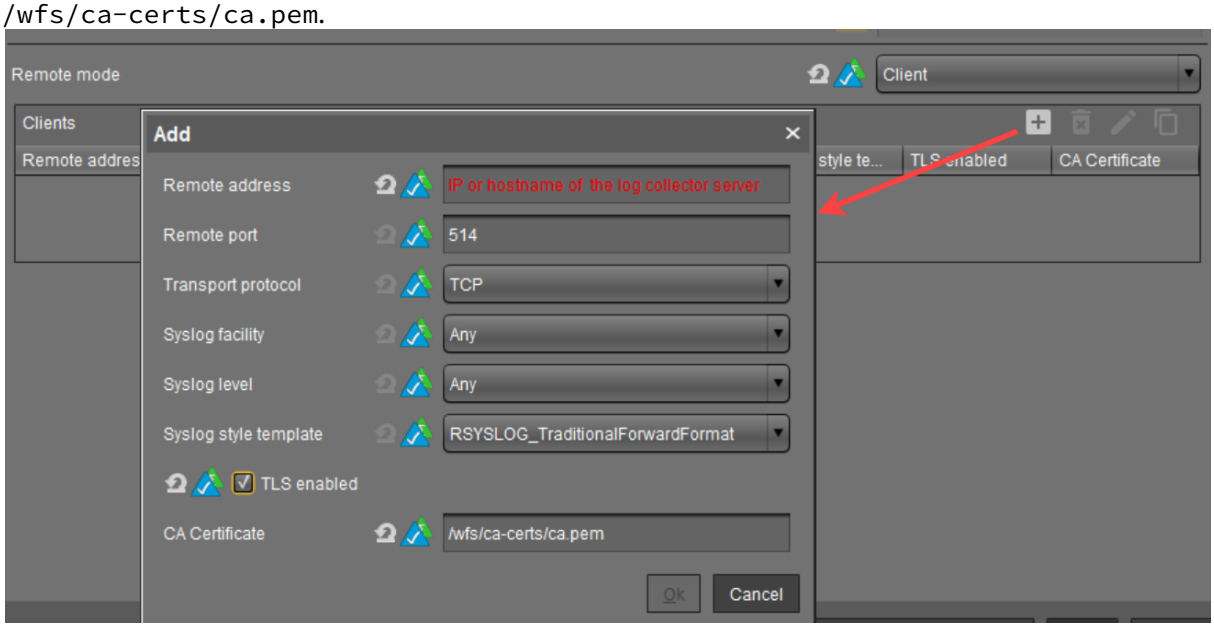
Configuration of Log Forwarding on IGEL OS

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[50].



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`.



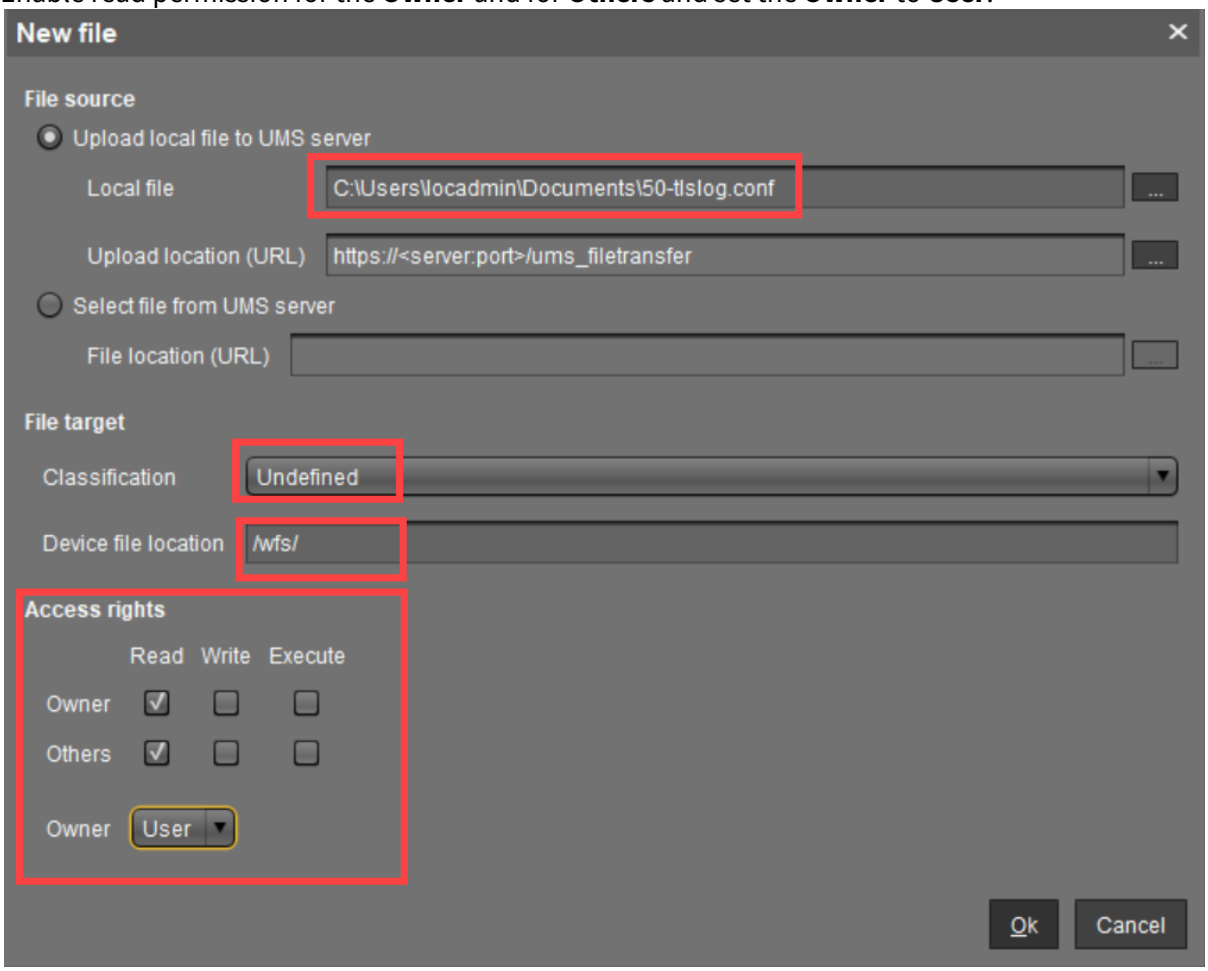
7. Save the changes and assign the profile to the desired devices.
8. Reboot the devices to make the change effective.

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:

50 https://kb.igel.com/display/endpointmgmt608/Creating+Profiles

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**.

8.1.10 Datensicherung

This document is available in German only.

8.1.11 Verschlüsselung

8.1.12 Virenschutz

8.1.13 Systempflege

8.1.14 Zusätzliche Anforderungen aus SYS.2