WHITE PAPER

HOW TO SECURE ENDPOINTS WITH IGEL OS

igel.com

How to Maximize Endpoint Security with IGEL OS

A STEP BY STEP GUIDE

Purchasing and deploying security software is a top priority for CIOs*. Year after year CIO surveys cite security as one of their top priorities. Most organizations are challenged to keep up with both next generation tools and the sophistication of attacks and attack vectors. The weakest links in security are the endpoint and the end-user. IGEL's mission is a to deliver the highest performance and most secure endpoint, and help IT mitigate end-user mistakes.

How does IGEL deliver on this promise?

This paper is all about optimizing the features and functions that IGEL delivers to ensure the safety of the endpoint. At the core of this value proposition is a mature read-only 64-bit operating system and the ability for full granular, contextual policy based control of devices.

IGEL allows you to control over 7,000 settings, this can be challenging. This paper provides a recipe to put the full power of IGEL's security to work across your endpoints.

Windows vs. Linux: IGEL's philosophy is that Windows belongs in the datacenter where is can be effectively managed, protected from outside attacks, and can be optimized for application and desktop delivery. At the endpoint, in the hands of the end-users you need a rock solid, stable, secure and high performance OS tuned to deliver end-user productivity – eliminating the security and management challenges that Windows brings.

We hope you find this paper useful and please provide any feedback or questions you may have to info@igel.com.

*2017 AlphaWise CIO survey for Morgan Stanley.

WHITE PAPER

HOW TO SECURE ENDPOINTS SECURE IGEL OS

CONTENTS

Securing IGEL OS 10 Endpoints

This Best Practice document describes settings for IGEL OS that will increase security.

It applies to:

- **IGEL UD LX and IZ devices with IGEL OS version 10.01.100 and newer**
- **UD Pocket**
- **Devices converted with UDC3**

1.1. Introduction

This document describes various settings that will make IGEL OS more secure. In general the more of these settings you apply the better endpoint security will be. However, it is up to you to strike a balance between security and enabling your users to do their work. Some settings may even be inappropriate for your use case, e.g. if you use Bluetooth peripherals it does not make sense to disable Bluetooth.

In order to configure more than one thin client, put one or more settings presented here into a Universal Management Suite (UMS) master profile, which you can assign to any number of thin clients, enforcing the security settings.

Learn more about using master profiles in the IGEL UMS 5 Profiles Reference Manual (http://edocs.igel.com/manuals/en/en_prof/index.htm).

Setting Passwords

You can restrict access to various system components by setting passwords.

1.1.1. Setting Local Passwords

Rationale

Passwords protect the system against local changes. They restrict access to the Local Terminal, Setup and to the rescue shells on the virtual consoles. The administrator password is also needed to reset the system to factory defaults.

These passwords are saved in a way (salted and hashed) that prevents recovering them from the local storage.

Instructions

By default, no passwords are set on IGEL OS. Set at least an administrator password:

1. In IGEL Setup go to **Security > Password**.
2. In the Administrator area check **Use Password** and enter a password twice when prompted.
3. Optional: If you want to grant an unprivileged user access to IGEL Setup check **Use Password** in the **Setup user** area and enter a password twice when prompted.
4. Click **Apply**.

For configuring the User Account for Remote Access, see Using Secure SSH Settings (p19).

Find further information on the Passwords page in the IGEL OS manual. (http://edocs.igel.com/index.htm#11506.htm)

1.1.2. Password-Protecting Sessions and Accessories

Rationale

Sessions can be used to access corporate resources, the accessories in IGEL OS can be used to make changes to the local system. If you do not want to disable certain sessions or accessories completely, you can set passwords to restrict access to them.

Instructions

By default, sessions do not have passwords set. To enable password protection for a session, follow these instructions:

1. In IGEL Setup go to **Sessions > [session type] > [session name] > Desktop Integration.** For accessories, go to **Accessories > [accessory name]**.
2. Set **Password Protection** to
   - **Administrator** to require the Administrator password, or
   - **User** to require the User password, or
   - **Setup User** to require the Setup User password.
3. Click **Apply**.

1.1.3. Using Screen Lock

Rationale

Leaving a screen unlocked enables attackers to access the system with the logged-in user's privileges. Manually or automatically locking the screen with a password set prevents this.

Instructions for Enabling Manual Locking

By default, there is no way for the user to manually lock the screen. To enable manual locking, follow these steps:

1. In IGEL Setup go to **User Interface > Screen Lock/Saver**
2. Do one or both of the following:
   - Activate the **Quick Start Panel** starting method to give the user a button for locking the screen manually.
   - Activate **Use Hotkey** and set a combination of keys that lets the user lock the screen manually, e.g. Ctrl-Shift-L
3. Click **Apply and send to thin client**.

Instructions for Automatic Locking

By default the screen saver is started automatically after 5 minutes, but the screen is not locked with a password. To enable locking, follow these instructions:

1. Go to **User Interface > Screen Lock/Saver > Options.**
2. Activate **Start automatically.**
3. Set the **Timeout**, i.e. the number of minutes of user inactivity before the screen saver starts automatically automatically. (Default: 5)
4. As a password select **User Password** (see Setting Local Passwords (page 4)) or a separate **Screen Lock Password** (and set one). (Default: none)
5. Optionally, check **Allow Administrator password** to allow the administrator to unlock a user's screen. (Default: enabled)
6. Click **Apply**.

1.1.4. Do Not Save Session Passwords

Rationale

Passwords for sessions should not be saved on the endpoint device.

Instructions

- When configuring a session, under Logon leave the Password field empty. The user will then be prompted interactively for the password.
- Wherever possible use Two-Factor Authentication (2FA).

1.1.5. Setting a UEFI Password

Rationale

In the UEFI settings you can modify very fundamental system properties, e.g. disable booting from USB. Access to these settings should be protected by a password.

Instructions for IGEL UD LX devices

By default no UEFI password is set on IGEL UD devices. To set a password, do the following:

1. Hold down the Del key (F2 key for UD2) while booting.

   The UEFI menu opens.
2. Using the arrow and return keys, go to **SCU**.

   The **Setup Utility** opens.
3. Using the arrow and return keys, go to **Security**.
4. With the arrow keys select **Set Supervisor Password**
5. Hit Return
6. Enter the desired UEFI password and hit Return
7. Enter the same UEFI password again and hit Return twice.
8. Hit F10 in order to save and exit.
9. Confirm **Exit Saving Changes?** by hitting Return

   The system boots, the UEFI settings are now password-protected

Instructions for 3rd-Party devices converted with UDC3

- Refer to the instructions of your BIOS/UEFI vendor

Alternatively, try pressing F12 (in general), F10 (Intel devices) or F9 (Hewlett-Packard devices) to access the BIOS/UEFI settings. If this does not work, try pressing Del , F1 or F2 during boot

1.1.6. Using Two-Factor Authentication (2FA)

Rationale

Two-factor authentication (2FA) combines two different factors to prove the user's identity, often a hardware device such as smartcard or smart token and a password or PIN. This improves protection against impostors, as they would have to gain both possession of the hardware device and knowledge of the password or PIN.

Instructions

Use two-factor authentication with a smartcard or smart token where possible. IGEL OS supports this for the following features - the links will take you to the IGEL OS Manual:

- Smartcard authentication for sessions (http://edocs.igel.com/index.htm#10203266.htm):
  - Citrix Legacy
  - Citrix Legacy with local logon window
  - Citrix Storefront
  - Citrix Xen Desktop Appliance Mode
  - Within RDP sessions
  - Horizon sessions
  - Web browser
- (Kerberos) Passthrough Authentication (http://edocs.igel.com/index.htm#10200947.htm)

1.2. Keeping the System Up-to-date

Rationale

Software updates fix newly discovered vulnerabilities in IGEL OS and applications. Therefore keeping up with updates is one of the most important measures in securing IGEL OS systems.

Instructions

In order to be notified of security-critical IGEL OS updates, subscribe to the IGEL Technical Newsletter on **igel.com**.

You can use the Universal Firmware Update (http://edocs.igel.com/index.htm#9372.htm) feature in UMS to check for updates for your endpoint devices managed by UMS.

Test an IGEL OS update on one or more sample devices to see whether all features you require work, before you roll the update out to production.

1. Assign an update to one or more endpoint devices:
   - In UMS drag and drop a Universal Firmware Update (http://edocs.igel.com/index.htm#2285.htm) onto a device or a directory to assign the update.

   OR

   - In IGEL Setup go to **System > Update > Firmware Update** and configure an update source (http://edocs.igel.com/index.htm#11112.htm).

2. Launch the update process:

   - Manually: In UMS right-click a device or a directory and select **Update & snapshot commands > Update** or **Update on Shutdown** from the context menu.

   OR

   - As a scheduled job in UMS:

     a. Right-click Jobs in the navigation tree.

     b. Select **New Scheduled Job**.

     c. Enter a **Name**.

     d. Select **Update, Update on Boot** or **Update on Shutdown** as the **Command.**

     e. Complete the configuration of the task, see Details (http://edocs.igel.com/index.htm#9383.htm).

     f. Assign (http://edocs.igel.com/index.htm#3029.htm) the task to thin clients or directories.

Disabling Access to Components

You can hide IGEL OS components from the user that could be used to make changes to the system.

1.2.1. Disabling Local Terminal Access

Rationale

The Local Terminal accessory allows the user to execute commands or make changes to the system. Leave it disabled.

Instructions

By default the user does not find a Local Terminal session in the Start Menu or on the Desktop. To remove an existing Local Terminal session:

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

→ Alternatively, you can password-protect the Terminal.

1.2.2. Disabling Virtual Console Access

Rationale

The virtual consoles `tty11` and `tty12` give the user access to a shell. Disabling these makes it more diffcult to execute commands or make changes to the system.

Instructions

By default, the user can access the virtual consoles with the Ctrl + Alt + F11 and Ctrl + Alt + F12 keyboard commands. To disable access, do the following:

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

1.2.3. Using Appliance Mode

Rationale

In Appliance Mode a single predefined session is presented fullscreen to the user. As access to other applications is prevented, this reduces the system's attack surface.

Instructions

By default IGEL OS users are not presented with a fullscreen remote session, but have access to the Desktop and the Start Menu. To enable Appliance Mode, follow these instructions:

1. In IGEL Setup go to **Sessions > Appliance Mode.**
2. Pick a session and configure it:

   - VMware Horizon
   - Citrix XenDesktop
   - Citrix Self-Service
   - RHEV/Spice
   - Imprivata
   - RDP MultiPoint Server
   - Caradigm

   → Find instructions in the Appliance Mode (http://edocs.igel.com/index.htm#10973.htm) section of the IGEL OS Manual.

You can combine most of the Appliance Mode sessions with Two-factor Authentication for increased security.

1.2.4. Hiding Unused Accessories

Rationale

Accessories can be used to make changes to the system. Restricting access to these help keep the system secure.

Instructions for the Start Menu

By default the user finds a wide selection of accessories in Start Menu's System Tab.To hide individual accessories (both in the Start Menu and the Application Launcher):

a. In IGEL Setup go to **Accessories > [accessory name].**

b. Disable all **Starting Methods for Session.**

c. Click **Apply**.

→ Alternatively, password-protect the accessory.

To hide the complete Start Menu's System Tab, which contains the accessories:

a. In IGEL Setup go to **User Interface > Desktop > Start Menu**.

b. Uncheck **Enable System Tab**. (Default: enabled)

c. Click **Apply**.

Instructions for the Application Launcher

A wide selection of accessories is also found in the System Tab of the Application Launcher. To hide individual accessories (both in the Start Menu and the Application Launcher):

a. In IGEL Setup go to **Accessories > [accessory name]**.

b. Disable all **Starting Methods for Session.**

c. Click **Apply**.

→ Alternatively, password-protect the accessory

To hide the complete Application Launcher's System Page, which contains the accessories:

a. In IGEL Setup go to **Accessories > Application Launcher > Application Launcher Configuration**

b. Activate **Hide system page** (Default: visible)

c. Click **Apply.**

Minimizing the Attack Surface

Removing unused features and disabling unneeded network services minimizes the parts of the system that can be attacked.

1.2.5. Removing the Local Web Browser

Rationale

The local web browser may expose vulnerabilities to the Internet and can be an entry point for malware. If it is not needed, it is safer to remove it.

Instructions

By default, IGEL OS has a local web browser (Firefox) installed, even if no web browser session is configured. To remove the browser, follow these instructions: In the IGEL Setup go to System > Firmware Customization > Features. Uncheck the Local Browser (Firefox) feature. Click Apply. Reboot the endpoint device.

1.2.6. Configuring the Browser (Kiosk Mode)

Rationale

If you want to offer a local web browser there are some settings that improve its security. Additionally, these settings add up to a kiosk mode, hiding the rest of IGEL OS from the user.

Instructions

By default the web browser makes all of its features and menus available. To achieve a restricted ‘kiosk’ mode, follow these instructions:

1. In the IGEL Setup go to **Sessions > Browser > Browser Global > Security**
2. Activate **Safe Browsing** (Default: deactivated)
3. Activate **Malware Protection** (Default: deactivated)
4. Go to **Sessions > Browser > Browser Sessions > [session name] > Settings > Restart**
5. Enable **Autostart** (Default: deactivated)
6. Enable **Restart** (Default: deactivated)
7. Go to **Sessions > Browser > Browser Sessions > [session name] > Window**
8. Enable **Start in Fullscreen Mode** (Default: deactivated)

9. Enable **Hide local filesystem** (Default: deactivated)
10. Enable **Hide configuration page of the browser** (Default: enabled)
11. Go to **Sessions > Browser > Browser Sessions > [session name] > Settings > Menus & Toolbar**
12. Activate **Hide App Menu/Menu Bar (Default: deactivated)**
13. Go to **Sessions > Browser > Browser Sessions > [session name] > Context**
14. Check **Hide the browser's context menu** (Default: deactivated)
15. Click **Apply.**
16. Reboot the endpoint device.

1.2.7. Disabling Java in the Browser and JWS

Rationale

Java is a powerful programming language that can harm your data and system. Disabling the Java plugin in the web browser and Java Web Start (JWS) protects you from executing Java programs from the Web.

Instructions

By default, both the Java plugin in the web browser and Java Web Start are activated. Here is how to deactivate them:

1. In the IGEL Setup go to **System > Registry**
2. Go to the **java.deployment.webjava_enabled Registry key.**
3. Uncheck **Enable Java content in the browser.**
4. Click **Apply.**
5. Reboot the endpoint device.

1.2.8. Disabling the PC/SC Daemon

Rationale

Unless you are running smartcard readers that use it, you can disable the PC/SC daemon. Running less daemons reduces the attack surface.

Instructions

By default, the PC/SC daemon is activated. Follow these steps to deactivate it.

1. In the IGEL Setup go to **Security > Smartcard > PC/SC**
2. Uncheck **Activate PC/SC Daemon** (Default: Activated).
3. Click **Apply**.

Do not disable the PC/SC daemon if you use smartcard readers that rely on it.

1.2.9. Disabling X Server TCP Connections

Rationale

The X graphics server in IGEL OS has network functionality that could allow others to see your screen and read keyboard input. Leave it disabled to keep your data confidential.

Instructions

By default the network functionality of the X server is disabled. To disable it again at a later time, do the following:

1. In IGEL Setup go to **User Interface > Display > Access Control**
2. Make sure that **Access Control** is enabled (default)
3. Make sure that **Disable TCP connections is** checked (default)
4. Click **Apply**.

1.2.10. Removing Unused Features

Rationale

Reducing the amount of software running on a system reduces its attack surface. Therefore a basic security measure for IGEL OS 10 is to remove all unused features.

Instructions

By default IGEL OS comes with a wide variety of features enabled. To disable any of these, do the following:

1. In the IGEL Setup go to **System > Firmware Customization > Features.**
2. Uncheck all the features that you do not use.

   If you do not use local printers on the endpoint device that you want to share with others, uncheck:

   - **Printing (Internet Printing Protocol CUPS)**
   - **Printing (Line Printer LPD)**
   - **Printing (TCP/IP)**
   - **Printing (ThinPrint)**

Do not remove the Custom Partition feature if you have a custom partition that contains software or data that you have no backup copy of. After disabling the feature and a reboot the contents of the custom partition will be lost.

Do not remove Fluendo Gstreamer Codec Plugins or Hardware Video Acceleration if you use sessions that make use of these features, see the FAQ IGEL Linux Features that require the Multimedia Codec-Pack (http://edocs.igel.com/index.htm#10200858.htm).

3. Click Apply.

4. Reboot the endpoint device.

1.2.11. Disabling Storage Hotplug

Rationale

Removable USB media can be used to steal data or to execute unallowed software or even malware on the endpoint device.

Instructions

Storage Hotplug is disabled by default. Should you want to disable it again at any later point, follow these instructions:

1. In IGEL Setup go to **Devices > Storage Devices > Storage Hotplug**.

2. Uncheck **Enable dynamic client drive mapping** (Default: disabled)

3. Set **Number of storage hotplug devices to** 0 (Default: 0)

4. Click **Apply**.

Storage devices are now no longer automatically mounted when they are plugged in.

1.2.12. Using USB Device Control

Rationale

USB devices such as pen drives, wireless controllers or printers can be used to steal data or to execute unallowed software or even malware. Deactivating as many USB device classes as possible increases security.

Instructions

By default USB access control is not active. To enable and configure it follow these steps:

1. In IGEL Setup go to **Devices > USB access control.**

2. Check **Enable**.

3. Set **Default rule** to **Deny**.

4. Click **Apply**.

5. Reboot the endpoint device.

In combination with the preconfigured rule that allows Human Interface Devices (HID), no USB devices apart from e.g. mouse and keyboard are allowed.

1.2.13. Disabling USB Boot

Rationale

Disabling USB boot prevents booting another operating system, which could be used to manipulate or (even accidentally) overwriting IGEL OS on mass storage.

Instructions for IGEL UD LX Devices

USB boot is disabled in the factory settings on IGEL UD LX devices. If you want to disable it at any time in the devices lifetime, here are the instructions:

1. Hold down the Del key (F2 key for UD2) while the system is booting. The UEFI menu opens.

Instructions for IGEL UD LX Devices

USB boot is disabled in the factory settings on IGEL UD LX devices. If you want to disable it at any time in the devices lifetime, here are the instructions:

1. Hold down the Del key (F2 key for UD2) while the system is booting. The UEFI menu opens.
2. Using the arrow and return keys, go to **SCU.**
3. Optional: Enter the UEFI password (if one is set).

   The **Setup Utility** opens.
4. Go to **Boot**.
5. Set USB Boot to Disabled.
6. Press F10
7. Confirm **Exit Saving Changes?**
8. The device boots.

Additionally, set a UEFI Password so the boot settings cannot be changed back.

Instructions for 3rd-Party devices converted with UDC3

→ Refer to the instructions of your BIOS/UEFI vendor

Alternatively, try pressing F12 (in general), F10 (Intel devices) or F9 (Hewlett-Packard devices) to access the BIOS/UEFI settings. If this does not work, try pressing Del , F1 or F2 during boot

Configuring Remote Access and Management

Remote management via UMS and remote access are powerful features of IGEL OS. Select secure settings and disable what you do not use.

1.2.14. Tying Endpoints to Your UMS instance

Rationale

Endpoint devices that have Remote Management enabled but are not yet tied to a UMS instance can be taken over by an attacker's UMS. Make sure to register all IGEL endpoint devices on your network

Instructions

By default Remote Management is enabled on IGEL OS endpoints. Use Autoregistration to catch all endpoint devices in your corporate network:

1. Assign the DNS entry `igelrmserver` to the UMS host.
2. In UMS Console go to **UMS Administration > Global Configuration > Thin Client Network Settings.**
3. Activate **Enable automatic registration (without mac address import)**

   Now all new IGEL thin clients and devices converted with UDC3 booting up on the network will automatically register with your UMS instance.
4. Optionally, put newly registered endpoint devices into a quarantine directory automatically with UMS Default Directory Rules (http://edocs.igel.com/index.htm#9531.htm).
5. Optionally, assign a Master Profile (http://edocs.igel.com/manuals/en/en_prof/index.htm) to this directory, enforcing secure settings, e.g. a local Administrator password.

Alternatively you can disable Remote Management in the local IGEL Setup under **System** > **Remote Management**. Of course this means losing one of the most powerful features of IGEL OS. However, for individual endpoints this is an option.

1.2.15. Disabling Shadowing

Rationale

Shadowing is made possible by a VNC server on IGEL OS, which is a network service. Reducing the number of running network services reduces the system's attack surface.

Instructions

By default Shadowing is not active on IGEL OS. However, if you want to disable it at any time, follow these steps:

1. In the IGEL Setup go to **System > Remote Access > Shadow**
2. Deactivate **Allow Remote Shadowing**.
3. Click **Apply.**

1.2.16. Using Secure VNC Settings

Rationale

If you intend to use shadowing on IGEL OS, there are a number of options that can make it more secure.

Instructions

By default Shadowing does not use encrypted network transport or a password. To activate these security features, do the following:

1. In IGEL Setup go to **System > Remote Access > Shadow**
2. Make as many of the following settings as possible for your use case. Each improves security, and often also privacy:
   - Enable **Secure Mode**.
   - Enable **Use Password** and set a strong password (not needed in **Secure Mode**)
   - Enable **Prompt User** to allow **Remote Session**.
   - Enable **Allow User to disconnect Remote Shadowing.**
   - Disable **Allow Input from Remote.**
3. Click **Apply.**

Secure mode for shadowing can be enabled globally in **UMS under UMS Administration** > **Global Configuration** > **Remote Access**. There you can also enable the logging of users who have used secure mode shadowing .

1.2.17. Disabling SSH Access

Rationale

The SSH server on IGEL OS is a network service. Reducing the number of running network services reduces the system's attack surface. Even more so in this case, as SSH by design enables a remote user to execute commands on the system.

Instructions

By default the SSH server is running on IGEL OS. To deactivate it, follow these steps:

1. In IGEL Setup go to **System > Remote Access > SSH Access.**
2. Uncheck **Enable.**
3. Click **Apply**.

1.2.18. Using Secure SSH Settings

Rationale

If you intend to allow SSH connections to IGEL OS, there are a number of options that can make these more secure.

Instructions In IGEL Setup go to **System** > **Remote Access** > **SSH**. Make as many of the following settings as possible for your use case. Each one improves security:

- Uncheck **Permit empty passwords**. (Default: deactivated)
- Uncheck **Permit administrator login**. (Default: deactivated)
- Deny **User access** for `user`, who can execute any command with regular user privileges. (Default: denied)
- Instead, allow **User access** for `ruser`, whose access is restricted by the list **Applications access for remote user** 'ruser'. (Default: allowed)
- Optional: Edit the list **Applications access for remote user 'ruser'**. It defines the commands that `ruser` can run from remote. (Default: a local shell and IGEL Setup).
- Click **Apply**.
- Go to **Security** > **Password**, under **User Account for Remote Access** activate **Use Password** and set a password
- Click **Apply**.

1.2.19. Disabling Secure Terminal

Rationale

The secure terminal server on IGEL OS is a network service, providing a TLS/SSL-encrypted Telnet session. Reducing the number of running network services reduces the system's attack surface. Even more so in this case, as Secure Terminal by design enables a remote user to execute commands on the system.

Instructions

By default Secure Terminal is not active. By default Secure Terminal is not active. Should you want to deactivate it at any time, do the following:

1. In IGEL Setup go to **System > Remote Access > Secure Terminal**
2. Uncheck **Secure Terminal.**
3. Click **Apply.**

Secure Terminal can be enabled globally in **UMS under UMS Administration** > **Global Configuration** > **Remote Access**. There you can also enable logging users of Secure Terminal.

Wi-Fi and Bluetooth

Rogue or unencrypted Wi-Fi access points can put your data at risk, and so can Bluetooth devices. If your endpoint device has Wi-Fi and Bluetooth, make sure to configure them securely or disable them.

1.2.20. Restricting Wi-fi Access

Rationale

Using an unencrypted Wi-Fi network or falling for a rogue access point puts your users' data at risk. Enable strong encryption and restrict Wi-Fi access to a default network and optionally a whitelist of additional networks in order to prevent this.

Instructions

By default Wi-fi is not activated on IGEL OS. To activate it and preconfigure one or more allowed networks, follow these instructions:

1. In IGEL Setup go to **Network** > **LAN Interface** > **Wireless**.
2. Check **Activate Wireless Interface**.
3. Do not check **Enable wireless manager**, as this would give the user free choice of Wi-Fi networks.
4. Click **Apply**.
5. Go to **Network** > **LAN Interface** > **Wireless** > **Default Wi-Fi network**.
6. Check **Enable WPA Encryption**.
7. Enter the Wireless network name (SSID).
8. Make authentication and encryption settings (see Default Wi-Fi Network in the IGEL OS Manual (http://edocs.igel.com/index.htm#11088.htm))
9. Click **Apply**.
10. Optional: **Configure Additional Wi-Fi networks**.

1.2.21. Disabling Bluetooth

Rationale

If your device has a Bluetooth interface it may be used to access data. Disabling it reduces the risk of data theft.

Instructions

By default Bluetooth is deactivated on IGEL OS. Should you want to disable it at any time, do the following:

1. In the IGEL Setup go to **Devices** > **Bluetooth**.
2. Disable **Activate Bluetooth**. (Default: disabled)
3. Click **Apply**.

1.3. Using UD Pocket for BYOD Devices

Rationale

Letting users access company resources with their own devices (BYOD) and software poses a security risk: These systems may have insecure configurations or even contain malware. In addition, company data should not be saved on users' private devices.

Instructions

Use UD Pocket. This ensures the use of secure and trusted software. As UD Pocket does not access the device's mass storage, company data and private data will remain separated.

2. Index

Visit us online at igel.com

IGEL
ENDPOINT MANAGEMENT

Revolutionary in its
Simplicity