SIM-CAP

CONTINUOUS NETWORK PACKET CAPTURE PLATFORM

USER MANUAL

English

sim-systems

SUMMARY

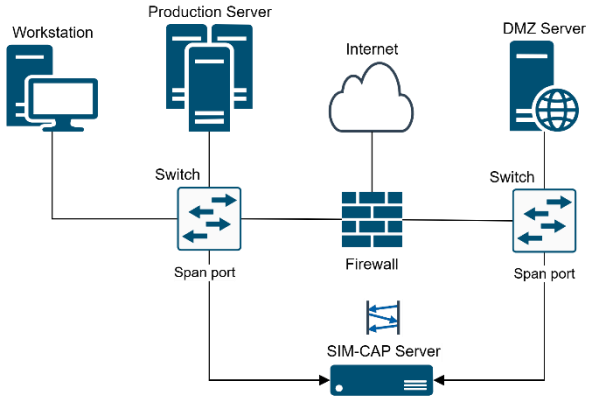
1. Overview

SIM-CAP is a platform for capturing, organizing, and managing network packets, developed to meet environments that demand high reliability, traceability, and efficiency in traffic analysis, especially in critical infrastructures and industrial networks.

Its main objective is to capture network packets in a continuous and structured way, organizing them in an intelligent way so that the user can easily retrieve, analyze and correlate information, using criteria such as date, time and associated capture process.

Operation concept

SIM-CAP was designed to be installed on a dedicated server, connected to the network infrastructure via port mirroring (SPAN). In this way, all traffic of interest can be copied to the capture server without interfering with the normal flow of the network.



From this point on, the system runs configurable capture processes, which store the packets in organized files, maintaining detailed metadata that allows the user to quickly identify:

- When the capture was made
- Which capture process originated it
- In which operational or investigative context does it fit

This model facilitates both daily operational use and deeper downstream analysis.

Capture Organization and Management

Unlike traditional point capture tools, SIM-CAP stands out for its centralized and structured management of the data collected.

Key features include:

- Indexing of captures by date and process
- Quick recovery of historical files
- Merging multiple captures into a single file
- Splitting large capture files into smaller chunks
- Packet filtering, allowing you to isolate specific traffic as needed by the user

These features make SIM-CAP especially suitable for environments with high traffic volume and data retention for long periods.

Protocols and use scenarios

SIM-CAP is widely applicable to the capture of communication protocols, with emphasis on industrial and automation environments, including but not limited to:

- IEC 60870-5-104 (IEC-104)
- DNP3
- Other TCP/IP and industrial protocols

In addition to operational use, the system is also a powerful tool for:

- Analysis of communication failures
- Traffic Audit
- Investigation and analysis of security incidents
- Forensic analysis of cyberattacks, allowing you to reconstruct events from historical captures

Web interface

All SIM-CAP management is performed through a web interface, accessible remotely through a browser, without the need to install additional client software.

Through this interface, the user can:

- Create and manage capture processes
- Track the status of captures in real time
- Browse and search historical captures
- Perform merge, filter, and split operations
- Centralize operational control of the system

The web interface is designed to be intuitive, secure, and suitable for continuous use in corporate and industrial environments.

Objective of SIM-CAP

In summary, SIM-CAP was designed to be a robust and scalable solution for capturing and managing network traffic, offering the user:

- Capture reliability
- Efficient data organization
- Ease of recovery and analysis
- Critical Environment Support and Advanced Investigations

2. Prerequisites

Before installing SIM-CAP, it is necessary to verify that the environment meets the minimum system requirements described below, ensuring the correct operation of the application and the stability of the capture processes.

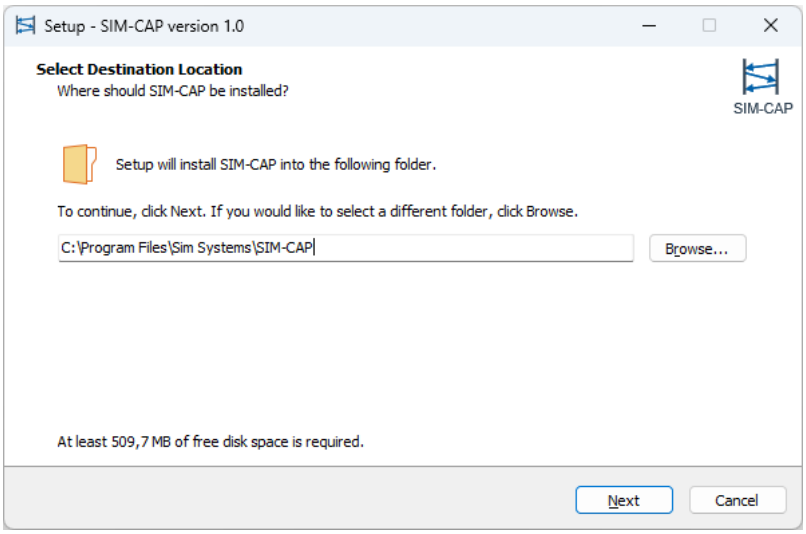
Requirement	**Specification**
Operating System	Windows 10+ Windows Server 2016+
CPU	x64 architecture
RAM Memory	2 GB
Disk Space	1 GB (excluding capture file space)
Web Browser	Google Chrome 64+ Mozilla Firefox 67+ Microsoft Edge (Chromium) 79+ Safari (macOS) 11+ Safari iOS 11+

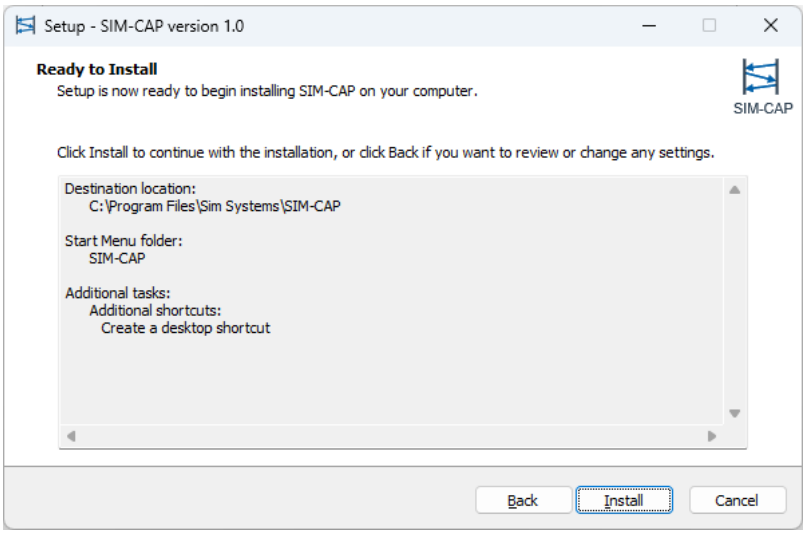
It is important to note that disk storage requirements can vary significantly based on the volume of traffic captured and the retention period configured. It is recommended that the disk space be properly sized according to the operational needs of the environment.

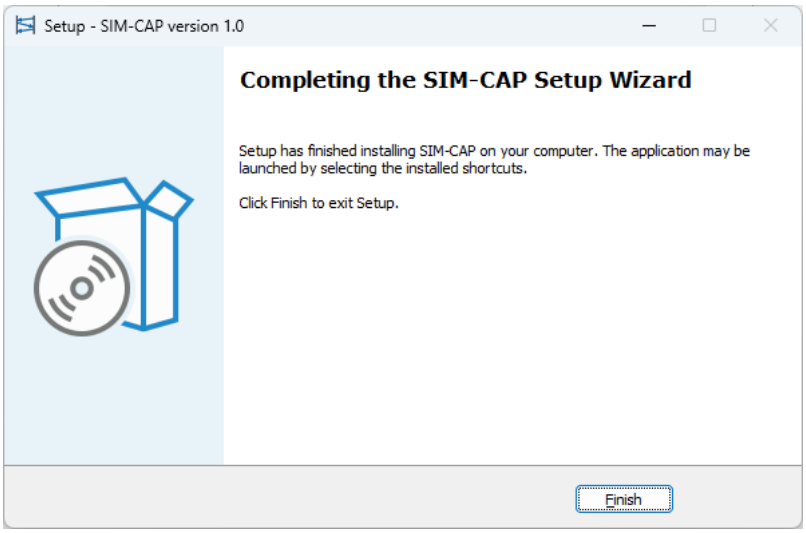
3. Installation

Software installation is simplified, follow the steps below:

- Run the installer.
- Click "Next" in subsequent windows.
- Click "Install" in the "Read to Install" window.
- Wait for the installation to be completed.

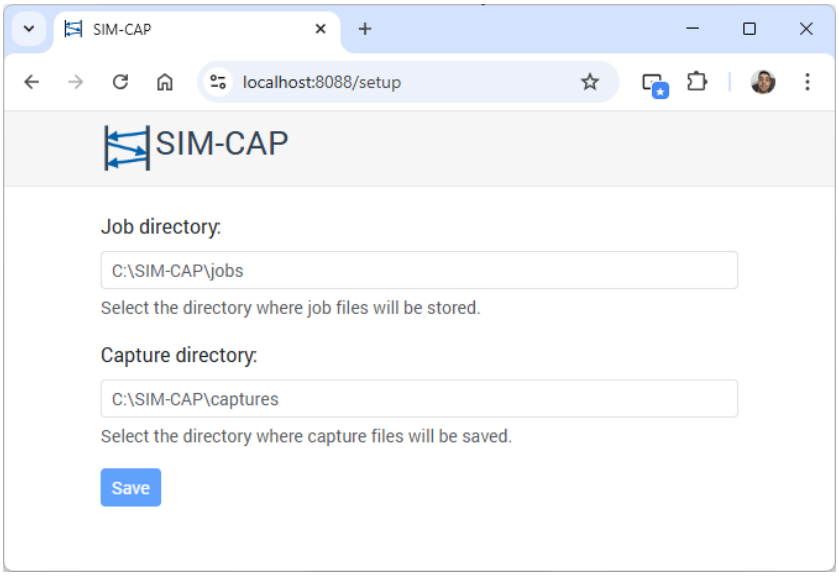





Setup - SIM-CAP version 1.0
Completing the SIM-CAP Setup Wizard
Setup has finished installing SIM-CAP on your computer. The application may be launched by selecting the installed shortcuts.
Click Finish to exit Setup.
Finish

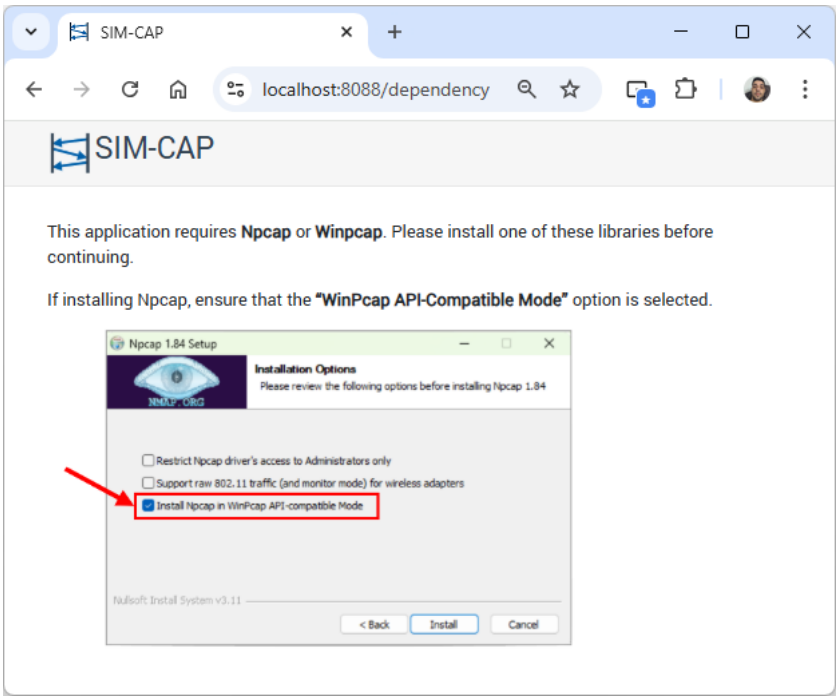
4. Initial settings

After installation, it is necessary to configure the directories for storing the Job files (Job Directory) and the capture files (Capture Directory).



A Job consists of a sequence of transformations applied to capture files, such as filtering, merging, and splitting, with the objective of generating one or more final files containing only the information of interest to the user. During the execution of these transformations, intermediate and temporary files are generated, which can result in high disk space utilization. For this reason, it is recommended to define a specific and dedicated directory for the storage of Job files.

The capture directory, in turn, is responsible for storing all the files generated by the capture processes, including historical data. Thus, it must be located on a storage device with adequate capacity for the estimated volume of traffic and the defined retention time. It is also recommended to use an exclusive partition independent of the operating system, to ensure better performance, security and predictability in the use of disk space.



After the directories are configured, a notification page may be displayed informing you of the absence of Npcap or WinPcap. This is because SIM-CAP relies on these libraries to perform network packet capture. Thus, it is mandatory that at least one of these libraries be installed before proceeding with the use of the application.

Libraries can be obtained from the following official addresses:

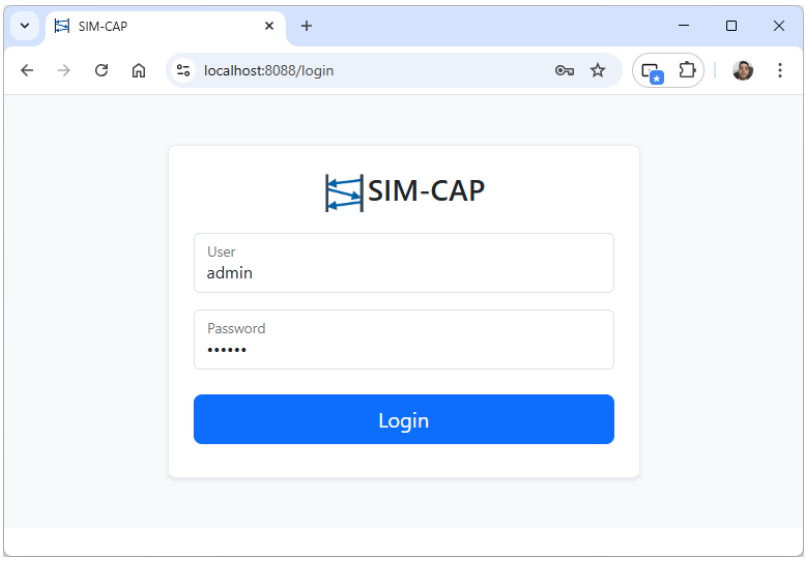
- NPCAP: https://npcap.com/#download
- WinPcap: https://www.winpcap.org/install

It should be noted that Npcap has its own licensing model when installed independently and is not subject to this restriction when included as part of the Wireshark installation.

If the installation of Npcap is chosen, it is essential to enable the "**WinPcap API-compatible Mode**" option during the installation process, ensuring compatibility with the capture mechanisms used by SIM-CAP, as indicated on the instruction screen displayed by the application.

5. Application access

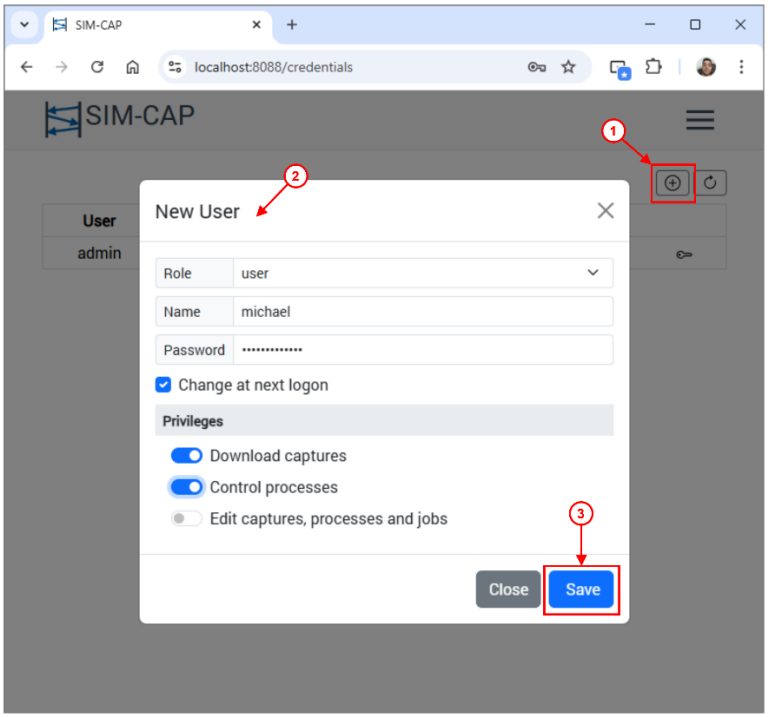
SIM-CAP has access control based on user and password authentication. Thus, on the first access to the application, the administrator must log in using the default administrator credentials, the user being "**admin**" and the password "**simcap**".



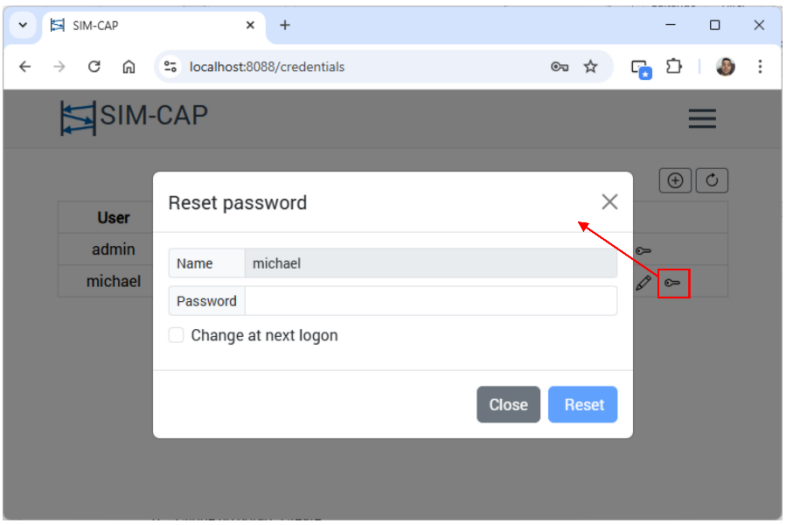
Once access to the system is granted, the administrator can, through the "Credentials" section, register new users and change their own password, a procedure that is highly recommended for security reasons.

To create a user, follow the instructions below:

1. Click the "Add" icon.
2. Fill in the fields requested in the "New User" form.
3. Click on the "Save" button to complete the registration.



To change the password of the admin user or any other registered user, click on the "Reset Password" button, as illustrated in the following figure.



6. Network and Firewall Settings

The system uses **TCP port 8088** by default for communication between the application server and clients.

It is imperative to ensure that port 8088/TCP is properly cleared at the operating system's firewall and any intermediary network devices, such as corporate firewalls, routers, or security appliances.

If the configured port is in use by another service, the application will not start correctly, and it will be necessary to adjust the configuration or release the port.

The default communication port can be changed through the "Settings" section of the application or directly in the settings.json configuration file, located in the "app/config" directory.

After any port changes, it is mandatory to restart the application server for the new configuration to take effect.

7. Capture process

The capture process is the task responsible for performing packet capture on a specific network interface, according to the previously configured parameters. Each process defines how, where, and what traffic data will be collected by SIM-CAP.

The following table describes the configurable parameters of a capture process:

Parameter	Description
Name	Capture process identifier name.
Interface	The network interface used to capture packets.
Filter	Berkeley Packet Filter (BPF) applied directly by the capture driver. This type of filter allows you to capture only specific traffic, significantly reducing the amount of data stored on disk. **Examples of BPF filters:** • tcp port 80 • src host 192.168.1 • host 192.168.1.0/24 • dst net 192.168.1.0 and tcp For more information on the syntax of BPF filters, please refer to the official documentation: • https://npcap.com/guide/wpcap/pcap-filter.html • https://www.winpcap.org/docs/docs_412/html/group__language.html
Files	Maximum number of capture files retained before the system automatically overwrites older files using a circular retention mechanism. It is recommended to set this parameter to balance historical retention and storage consumption.
File Size	Maximum size (in MB) of each capture file. When you reach this limit, a new file is automatically created. A value of **100 MB** is recommended to avoid excessive file generation and reduce overhead on analysis tools such as Wireshark.
Note	Field intended for observations or relevant information about the capture process.

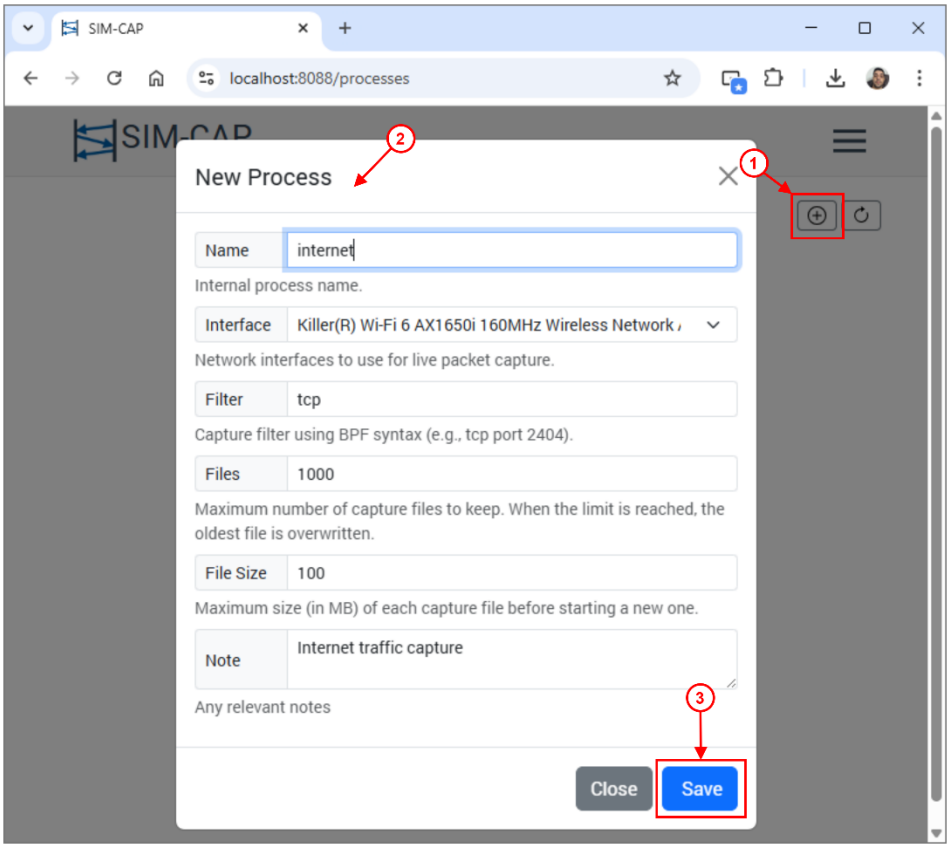
Circular File Retention

As defined by the "**Files**" and "**File Size**" parameters, SIM-CAP uses a circular-retained storage model, in which older capture files are automatically replaced with newer ones. This mechanism ensures the continuity of the capture, avoiding the interruption of the process due to lack of disk space.

Based on the average volume of traffic captured, you can estimate the retention period by adjusting the number of files and the maximum size of each file accordingly.

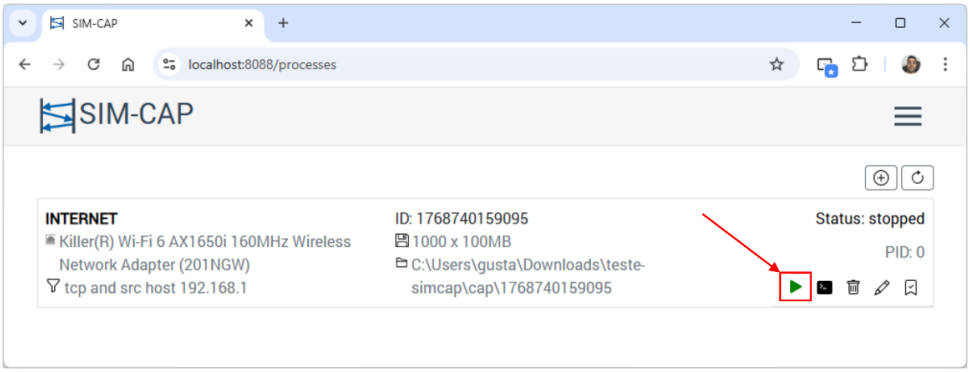
To create a capture process, follow these steps:

1. Click the "Add" icon.
2. Fill in the fields requested in the "New Process" form.
3. Click on the "Save" button to complete the registration.

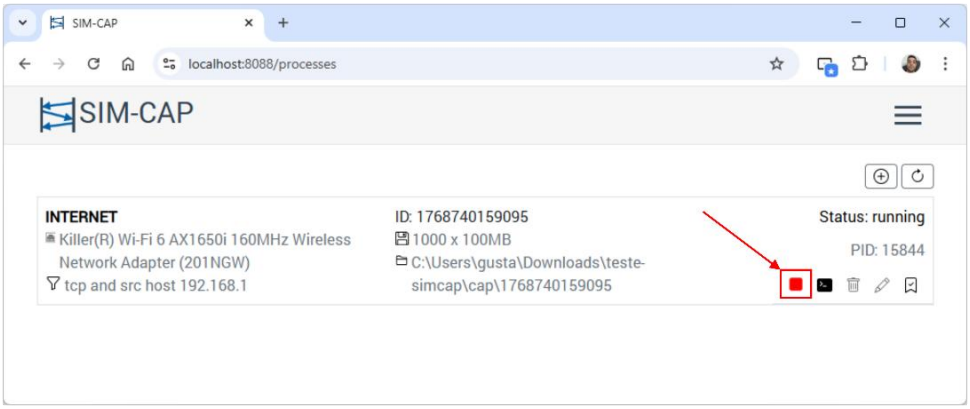


Only users with the "Edit captures, processes and Jobs" privilege can create capture processes.

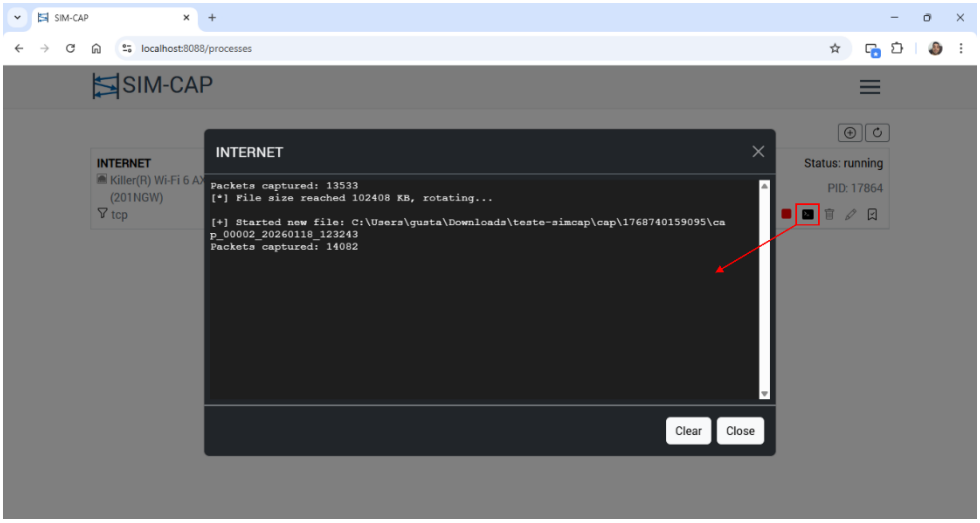
To start the capture process, click on the "Start" icon.



To stop the process, click on the "Stop" icon.

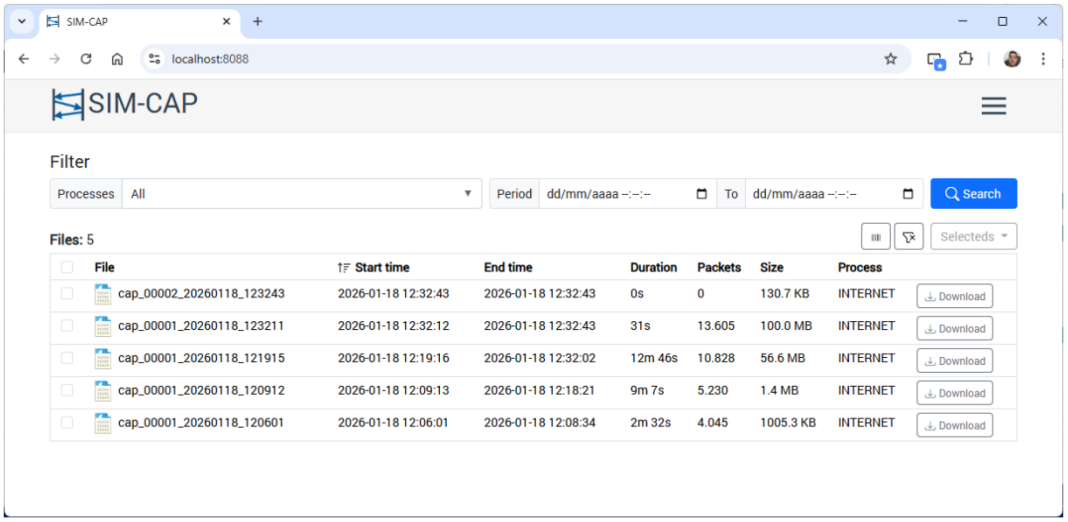


It is also possible to view the terminal output of the running process through the "Terminal" icon.



8. Captures and Jobs

The capture files generated by SIM-CAP are available in the "Captures" section. In this section, files can be searched and filtered based on the capture process and period of interest, as illustrated in the corresponding figure.



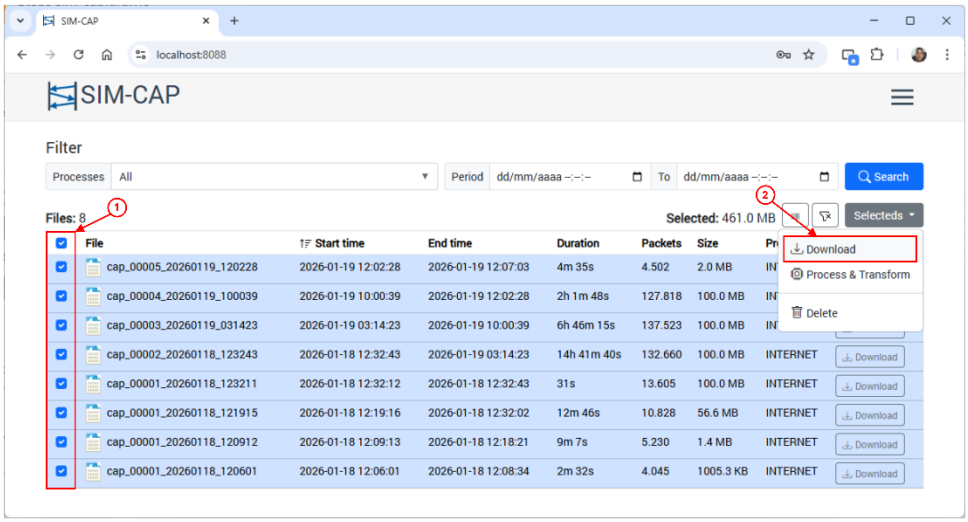
In addition to basic information such as start and end dates and times, the file list provides additional relevant data, such as capture duration and packet count, allowing for preliminary analysis before downloading or processing the files.

To download a single capture file, simply click on the "Download" button corresponding to the desired file.

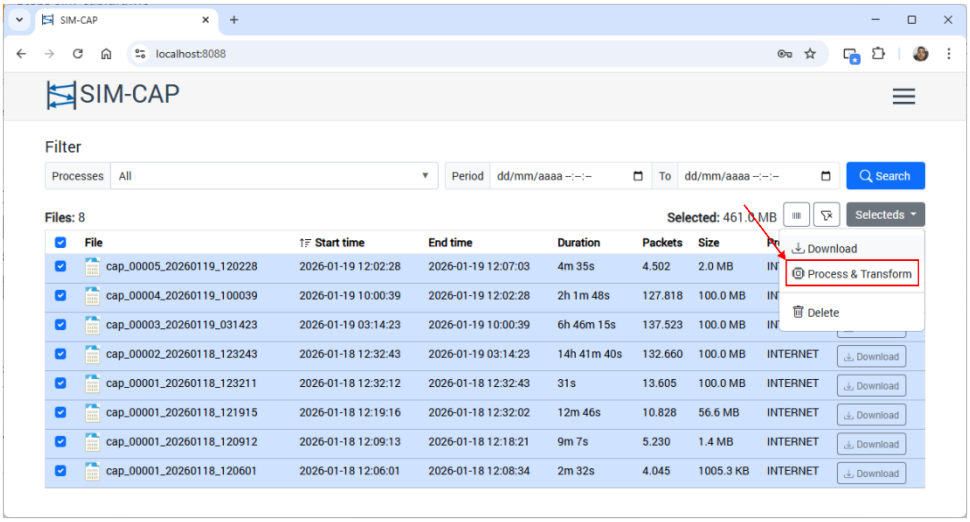
If multiple files need to be downloaded simultaneously, SIM-CAP allows for the automatic generation of a compressed file (zip). To do this:

1. Select the files of interest from the list.
2. Click on the "Download" menu from the "Selecteds" button.

The selected files will be consolidated into a single downloadable ZIP file.

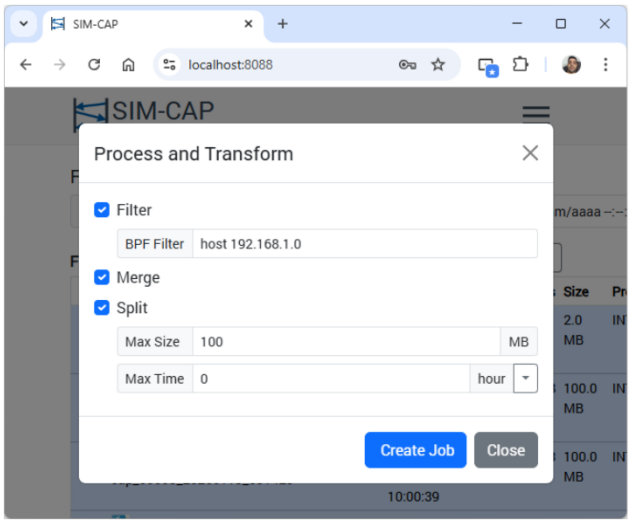


When there is a need to filter specific traffic, merge and/or split capture files, including those coming from different capture processes, select the "Process & Transform" option, as illustrated in the following figure.

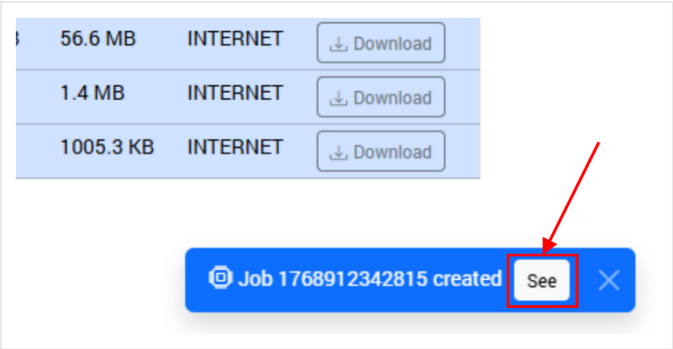


In this step, the user will be able to configure the desired transformations according to the objective of the analysis. In the example presented, a Job will be created that will perform the following actions:

- Filtering network packets that contain the 192.168.1.0 host.
- Merging the selected capture files in chronological order.
- Splitting the resulting file into multiple files with a maximum size of 100 MB.



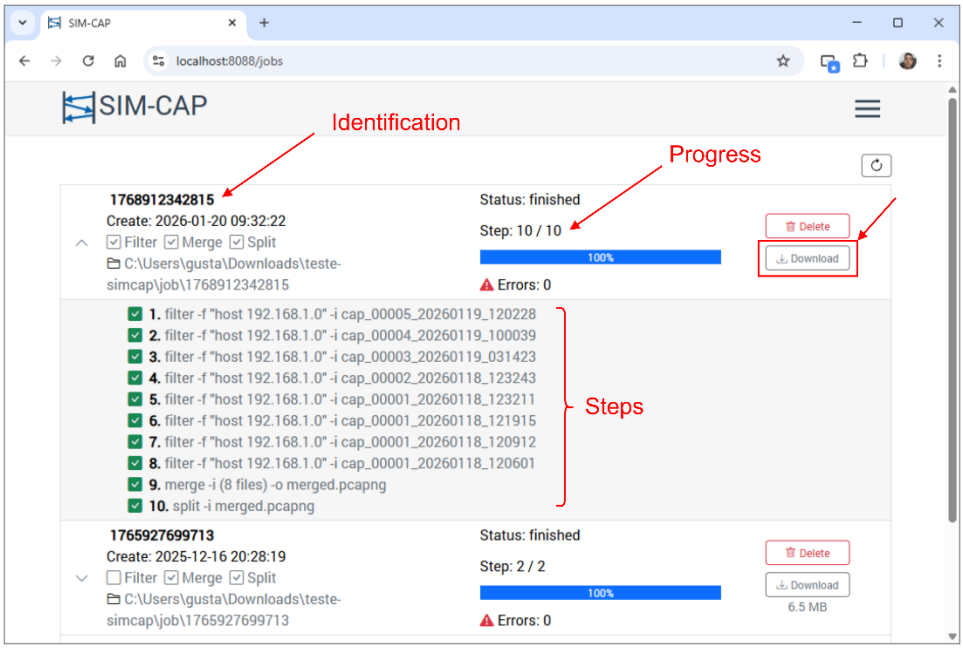
After the Job is created, a notification tooltip will be displayed in the bottom corner of the screen. By clicking on the "See" button, the user will be directed to monitor the execution of the Job, which can also be done by directly accessing the "Jobs" section.



In the "Jobs" section, detailed information about each Job is displayed, including:

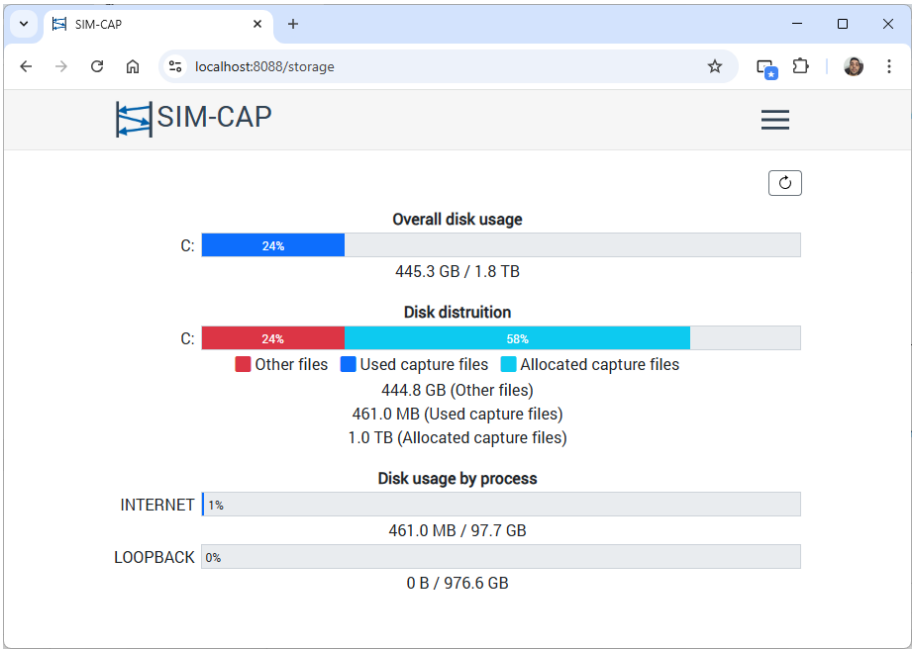
- Execution status
- Processing progress
- Steps taken

When the Job is completed, the "Download" button will be automatically made available, allowing access to the files resulting from the transformations.



9. Disk and storage usage

SIM-CAP provides disk usage monitoring functionality, allowing the administrator to visually and centrally monitor the system's storage utilization. The screen displays the total available space, the volume used, and the corresponding percentage, allowing a quick assessment of the overall disk occupancy.

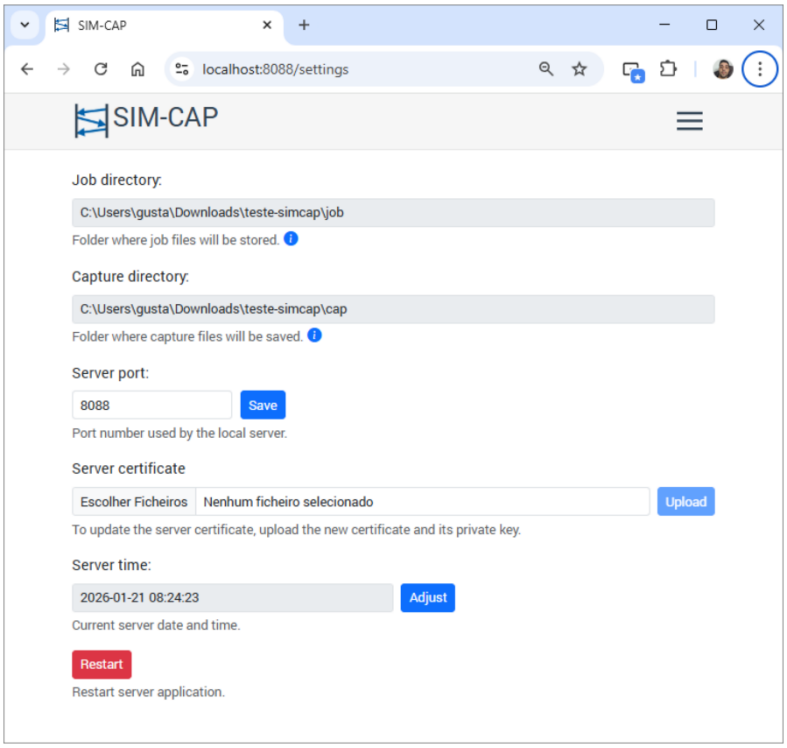


In addition to the overview, the system displays the distribution of disk usage, highlighting the separation between other files, capture files used, and the space allocated for captures. This visualization allows you to understand how storage is being consumed and reserved, evidencing the relationship between space effectively occupied and space previously allocated for capture processes.

Finally, SIM-CAP presents the disk usage per capture process, demonstrating, individually, the volume used and the total allocated for each configured process. This information helps to identify processes with the greatest impact on storage consumption and to adjust retention parameters, contributing to the continuity of captures and to the proper planning of disk capacity.

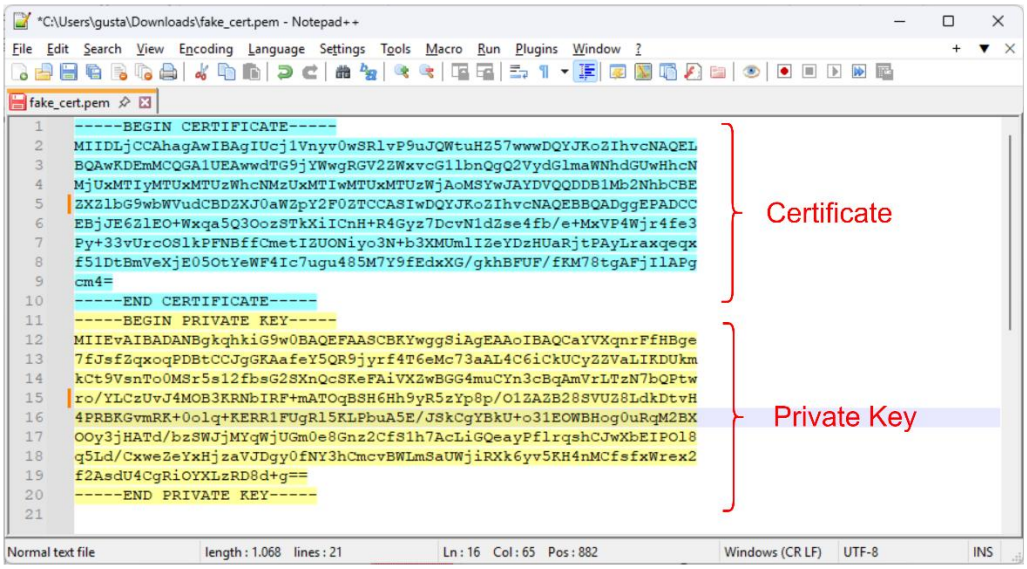
10. General Settings

In the "Settings" section, it is possible to consult some system settings and change others, as illustrated in the following figure. The main actions available in this section are changing the server's TCP port and updating the HTTPS security certificate.



To change the server's TCP port, simply modify the "Server port" field and click the "Save" button. Importantly, after this change, you must restart the server for the new configuration to take effect. The restart can be performed directly through the "Restart" button available on the interface itself.

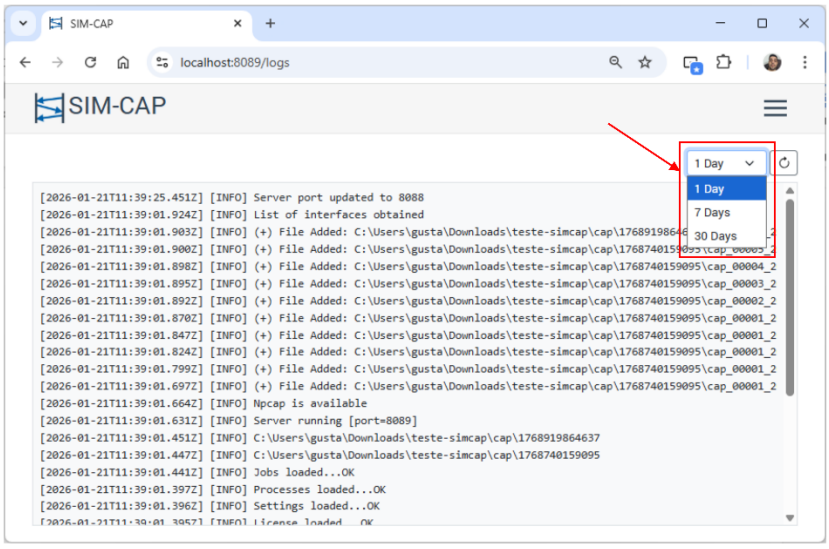
SIM-CAP is initially installed with a self-signed HTTPS certificate, which can cause the browser to indicate that the address is not secure. If the server is installed in an environment that allows validation by a certificate authority, it is possible to upload a new certificate using the "Server certificate" selector, and it is necessary to inform the certificate and the private key. If the certificate and private key are in separate files, both must be uploaded; If they are in the same file, a single upload is sufficient. In any situation, the application automatically checks for the presence of the start and end markers of the certificate and the private key.



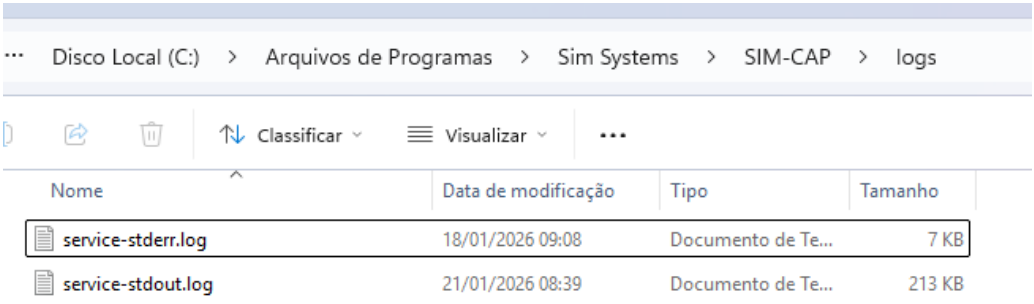
The settings for the capture and Jobs directories are displayed in this section for reference only. To change these settings, you need to access the "Setup" section via the URL "/setup". Still in the settings section, the server time is displayed, since the captures depend directly on the operating system clock and must be as accurate as possible. It is recommended that you use a time synchronization service, such as Windows NTP. The time update requires elevated privileges in the operating system, and, for this reason, the adjustment is not available directly through the SIM-CAP interface but must be performed in the operating system itself.

11. Logs

SIM-CAP has two sources of event logging (logs). The main one is the web interface, accessible through the "Logs" section, where the records are presented in a centralized and organized way. On this screen, the user can view the logs generated by the application, with the possibility of filtering by period, allowing the display of records corresponding to the last 1, 7 or 30 days, as illustrated in the following figure.



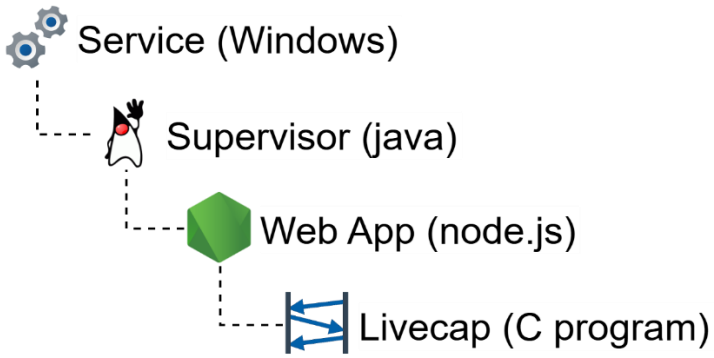
In addition to viewing via web interface, SIM-CAP also maintains logs generated by the supervisory application, which are stored in text file format. These files are available in the "logs" subdirectory, located in the program's installation directory, allowing offline analysis, audits or integration with external monitoring tools.



The joint use of these two log sources enables a complete analysis of the system's operation, facilitating the diagnosis of failures, the monitoring of capture operations and the verification of relevant events both in real time and historically.

12. Program structure

SIM-CAP was developed with a hierarchical application architecture, composed of different technological layers, including Java, Node.js and native applications developed in C, as illustrated in the following figure. This structure is designed to ensure operational robustness, continuous supervision, and isolation of responsibilities between system components.



The Windows service, called "SIMCAP," is the root element of the program's structure. It is through this service that SIM-CAP is started and ended in the operating system. When started, the Windows service runs the Java application, which acts as the system's control and supervision layer.

The Java application performs three main functions: license validation, web application initialization, and ongoing supervision of its operation. If the web application fails or interrupts unexpectedly, the Java module performs its automatic restart, acting as a watchdog mechanism, ensuring greater system availability.

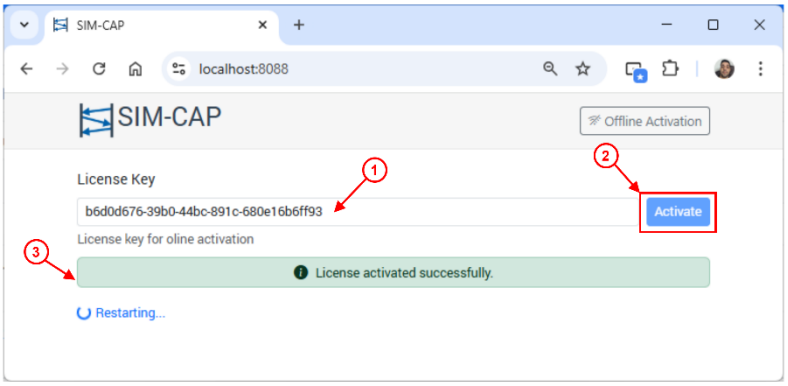
The application developed in Node.js is responsible for providing HTTPS services and constitutes the functional core of SIM-CAP. In addition to providing the web interface and management services, it directly controls the capture processes, which are executed through native applications developed in C. These processes correspond, in practice, to instances of the "livecap" executable and other auxiliary components. In total, SIM-CAP uses nine native executables related to network packet capture, transformation and management operations, ensuring high performance and efficiency in data processing.

13. Licensing

SIM-CAP is software licensed by Sim-Systems and, to fully use all its features, it is necessary to go through the licensing process. The system supports both online and offline licensing, also serving environments that do not have internet access.

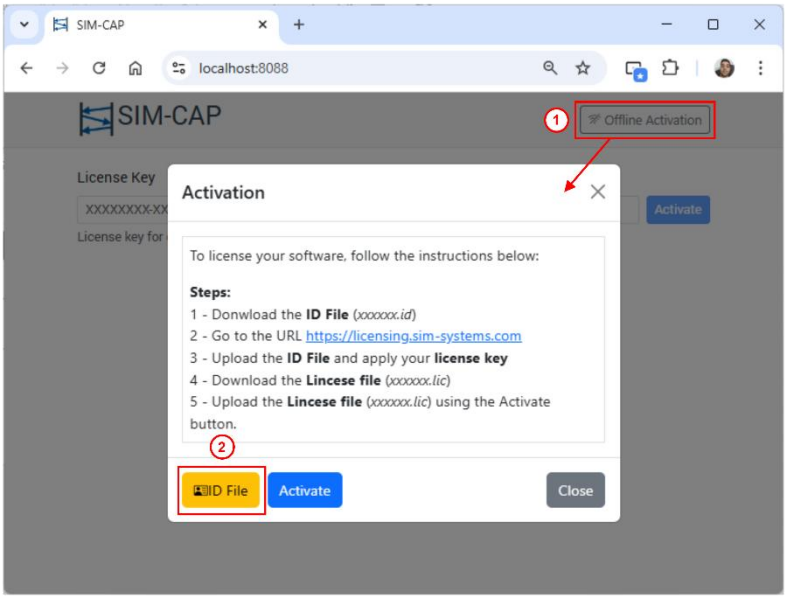
Online licensing is the simplest and most recommended method when the server has internet connectivity. To activate, follow the steps below:

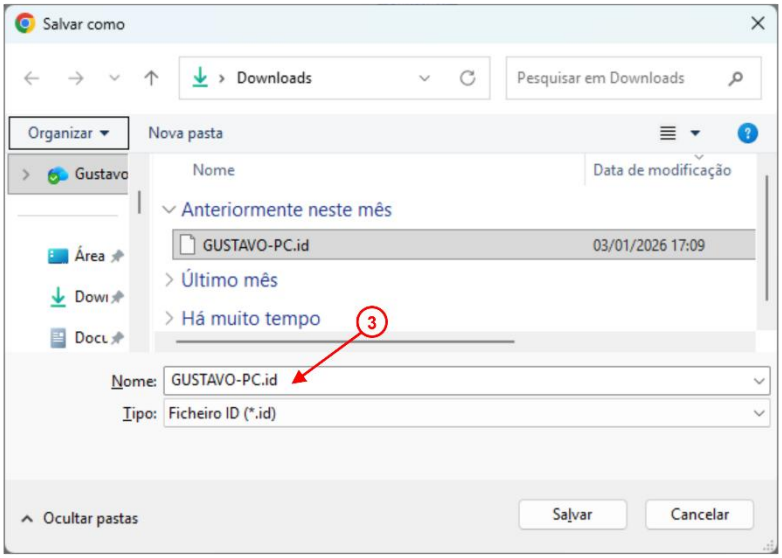
1. Fill in the "License Key" field with the purchased key.
2. Click on the "Activate" button.
3. Wait for the activation confirmation message and the application to restart.

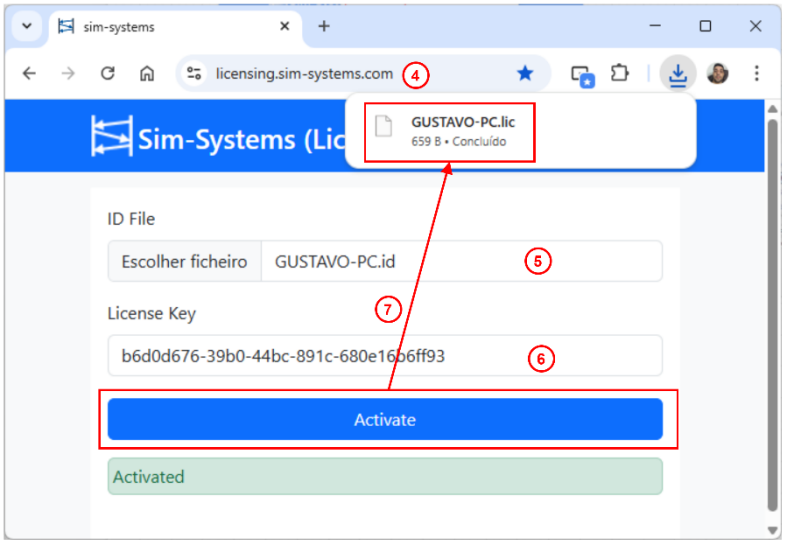


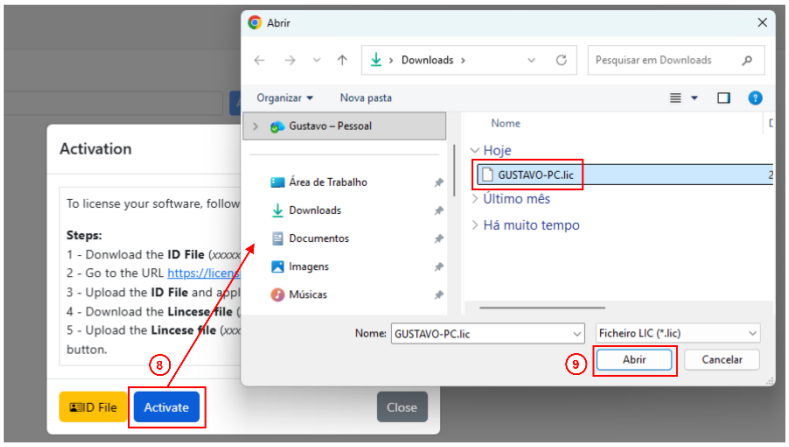
For offline licensing, perform the following steps:

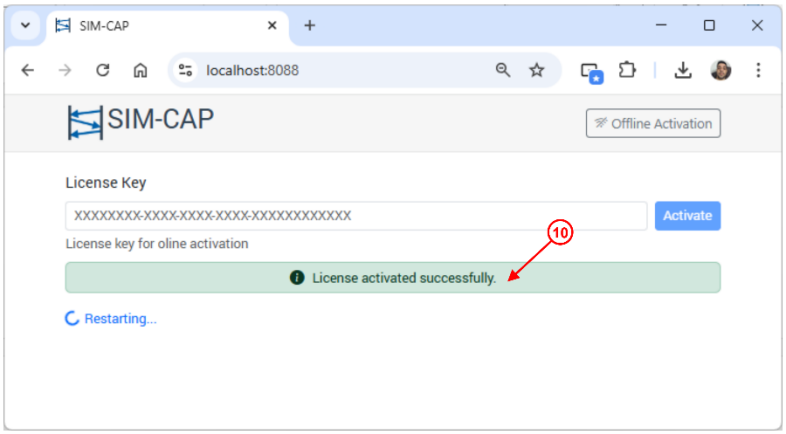
1. Click on the "Offline Activation" button.
2. Click on the "ID File" button.
3. Save the machine's identification file.
4. Access the webpage https://licensing.sim-systems.com.
5. Select ID file (.id).
6. Fill in the "License Key" field with the purchased key.
7. Click on the "Activate" button, then the license file (.lic) will be downloaded.
8. In the activation window, click on the "Activate" button.
9. Select the licensing file (.lic).
10. Wait for the activation confirmation message and the application to restart.


SIM-CAP
localhost:8088
SIM-CAP
1
Offline Activation
License Key
Activate
License key for
Activation
To license your software, follow the instructions below:
Steps:
1 - Donwload the ID File (xxxxxx.id)
2 - Go to the URL https://licensing.sim-systems.com
3 - Upload the ID File and apply your license key
4 - Download the Lincese file (xxxxxx.lic)
5 - Upload the Lincese file (xxxxxx.lic) using the Activate button.
2
ID File
Activate
Close


Salvar como
Downloads
Pesquisar em Downloads
Organizar
Nova pasta
Gustavo
Nome
Data de modificação
Anteriormente neste mês
GUSTAVO-PC.id
03/01/2026 17:09
Último mês
Há muito tempo
3
Nome: GUSTAVO-PC.id
Tipo: Ficheiro ID (*.id)
Ocultar pastas
Salvar
Cancelar


sim-systems
licensing.sim-systems.com
4
GUSTAVO-PC.lic
659 B • Concluído
Sim-Systems (Lic
ID File
Escolher ficheiro
GUSTAVO-PC.id
5
License Key
7
b6d0d676-39b0-44bc-891c-680e16b6ff93
6
Activate
Activated


Abrir
Downloads
Pesquisar em Downloads
Organizar
Nova pasta
Gustavo – Pessoal
Área de Trabalho
Downloads
Documentos
Imagens
Músicas
Nome
Hoje
GUSTAVO-PC.lic
Último mês
Há muito tempo
Nome: GUSTAVO-PC.lic
Ficheiro LIC (*.lic)
Abrir
Cancelar
Activation
To license your software, follow
Steps:
1 - Donwload the ID File (xxxxx
2 - Go to the URL https://licens
3 - Upload the ID File and appl
4 - Download the Lincese file (
5 - Upload the Lincese file (xxx
button.
ID File
Activate
Close
8
9


SIM-CAP
localhost:8088
SIM-CAP
Offline Activation
License Key
XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
Activate
License key for oline activation
License activated successfully.
Restarting...
10