



**ERMETIX**

## Datasheet

Ver 1.3

## Summary

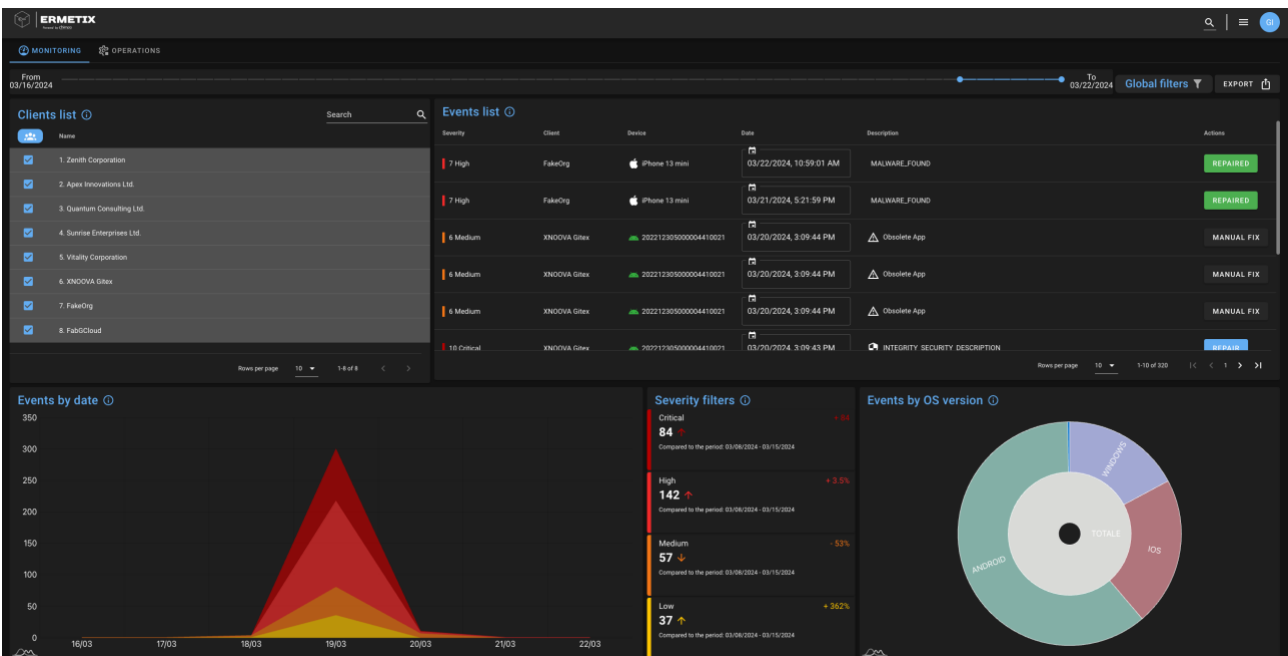
<b>Product Overview</b> .....	<b>2</b>
<i>Key Features</i> .....	2
<b>Security</b> .....	<b>3</b>
<i>Active Security</i> .....	3
Real-time Protection .....	3
Periodic Scans .....	3
<i>Offline Mode</i> .....	4
<i>Safe Browsing</i> .....	4
<b>Threat Intelligence</b> .....	<b>4</b>
<i>Behavioral Analysis</i> .....	5
Key Features of the Module .....	6
Logs and Analytical Data .....	6
<b>Passive Security</b> .....	<b>8</b>
<i>Risk Analysis and Non-Conformity Detection</i> .....	8
<i>Fully Configurable Policies</i> .....	9
<i>Data Analysis and Attack Prevention</i> .....	9
<b>Ermetix Web Console</b> .....	<b>10</b>
<i>Console Notifications</i> .....	10
Automatic and/or Manual Remediation .....	10
Advanced and Dynamic Filters .....	11
Device Inventory .....	11
Group-based Device Management .....	12
Data Visualization Based on Permissions .....	13
<b>Ermetix Agent on Mobile Devices</b> .....	<b>13</b>
<i>Device Notifications</i> .....	14
<i>Emergency Mode</i> .....	14
<i>Sharing Data on the Device</i> .....	15
<b>Additional Features</b> .....	<b>15</b>
<i>Sending Actions to the Device</i> .....	15
Actions related to apps & media: install or remove apps/APKs, upload or delete files. ....	16
Device-related actions: notification, reboot, shutdown, initialize. ....	16
<i>Installation of Configuration Profiles</i> .....	16
<i>Screen Lock Code Policy</i> .....	17
<i>Device Hardening</i> .....	17

# Product Overview

Ermetix is a powerful software solution designed to provide a comprehensive overview of mobile device inventory (Android, iOS, iPadOS, tvOS), as well as MacOS and Windows 10/11 devices, and their security posture.

With an intuitive and feature-rich dashboard, Ermetix enables users to visualize dynamic and filterable graphs and statistics.

Additionally, the software provides a detailed list of security events detected on various devices, allowing for in-depth analysis of threats and vulnerabilities.



## Key Features

Ermetix is a platform that allows monitoring, protecting, and managing the device fleet through a web console.

With simple and intuitive configuration, Ermetix can monitor and protect devices at three different security levels:

- Active (periodic anti-malware scans, real-time anti-malware protection, and secure browsing)
- Threat intelligence (behavioral analysis and IOC correlation)
- Passive (hardening of critical settings, known vulnerabilities, compliance rule configuration, patch management)

NAME	SERIAL	PRODUCT	DEP	STATUS	ACTIVE
iPhone	18C298B	OnePlus CPH2409	✓	Scanned	●
Device	R5C9T2L3N1CM	Samsung SM-A540B	✓	Scanned	●
iPhone	DRHFM89KP	iPhone 13 mini	✓	Scanned	●
Device	R9R602QH0Q	Samsung SM-T295	✓	Scanned	●
Device	HAI9HXVT	Lenovo TB-X306K	✓	Scanned	●
Device	4A4F3AD2E603	Xiaomi 2201119BUY	✓	Scanned	●
Device	2830295510CA02D5	Realme RMC3506	✓	Scanned	●
Device	56F92AB	Oppo CPH2343	✓	Scanned	●
iPhone11	38290LJH001N1	Google Pixel 8	✓	Scanned	●
Device	RFCW4206HSD	Samsung SM-S911B	✓	Scanned	●
Device	HVH55XYS	Lenovo TB-X306K	✓	Scanned	●

# Security

## Active Security

### Real-time Protection

Ermetix enables real-time monitoring of devices by analyzing potential malware whenever necessary. Specifically, scans are performed when:

- A file is downloaded/created, modified, or moved
- A folder is created, modified, or moved
- An app is installed

### Periodic Scans

Periodic scans are initiated every 24 hours from the initial anti-malware configuration. This type of scan covers the entire file system and installed applications, useful for detecting dormant malware and any malware present in the device firmware.

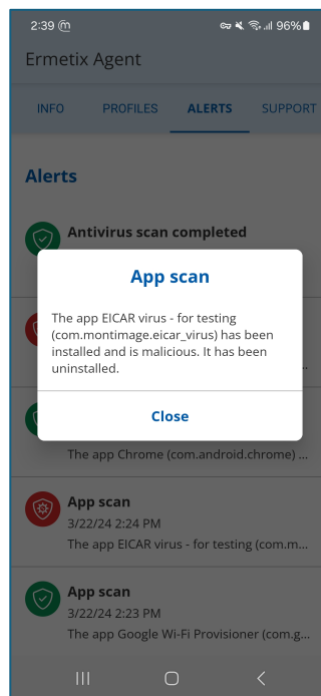
### Scan Details

Scans performed by Ermetix occur through specific applications for each operating system that:

- Monitor changes to all files in the file system and initiate an ad hoc scan whenever a file is added, modified, or moved, ensuring device security at all times.
- Recursively scan all folders affected by the above change
- Analyze each app as soon as it is installed and uninstall it if it tests positive for anti-malware scanning.

These types of scans are based on signatures that are periodically updated; this system component, therefore, works on known malware.

Signature updates are pushed from Ermetix to the device.



## Offline Mode

Devices are monitored even when offline thanks to signatures present on the device itself and algorithms executed to search for potential malware without known signatures. This feature is particularly useful in situations where the device cannot access the network, such as locations with no or poor internet connection.

If the device is offline, it cannot communicate scan data to the administration console; however, this data will be sent to Ermetix at the earliest opportunity.

For all detections, the system automatically remediates, and if automatic remediation is not possible, emergency mode can be activated (configuration available from the management console).

It should be noted that the initial configuration requires an internet connection to allow the device to download the necessary data for subsequent scans, as well as a connection to download signature updates.

## Safe Browsing

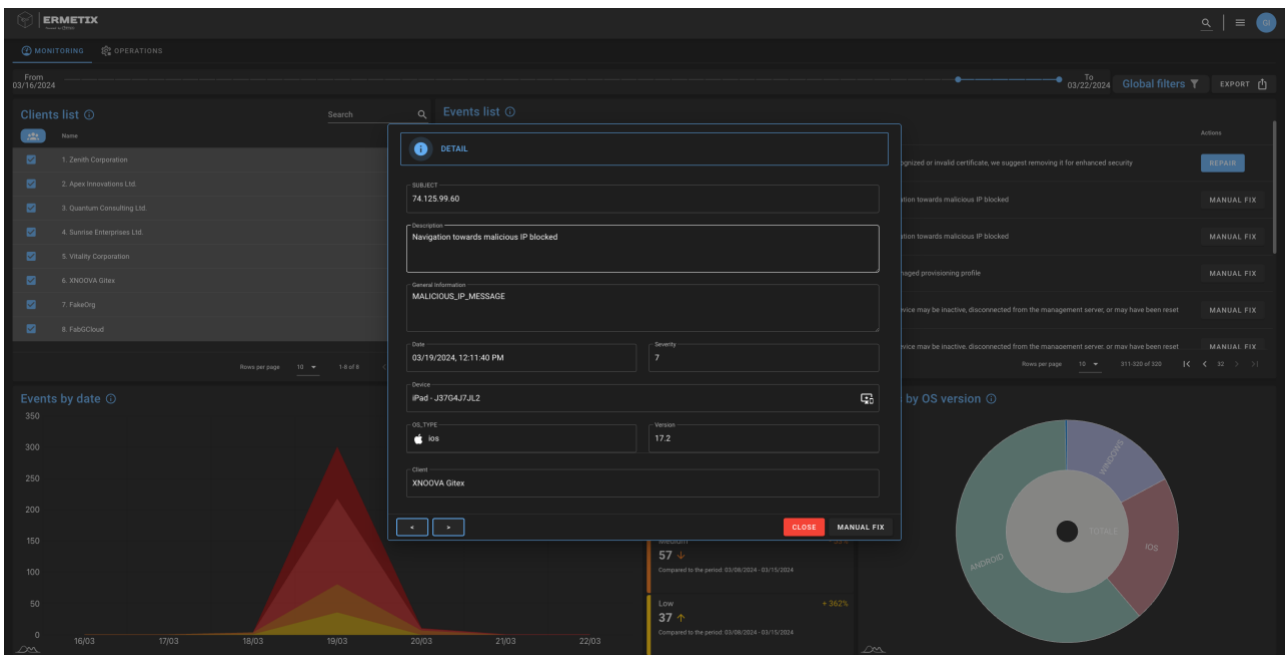
Ermetix allows users to browse safely; thanks to Safe Browsing protection, it is possible to prevent users from visiting potentially harmful websites and, secondly, prevent potentially malicious applications from contacting malicious IPs/domains.

This functionality is also useful if the device is not compliant with security policies: in this case, Ermetix can discard all network traffic packets (sinkhole).

Those viewing the management console can verify all resources blocked on the devices and block/permit browsing to preconfigured IPs/domains through allow-list and block-list mechanisms.

Ermetix also offers the option to use secure DNS for domain resolution.

In the image below, we can see how Ermetix's panel can easily identify addresses blocked by the Safe Browsing system; in this particular case, browsing to an IP associated with phishing activity has been blocked.



## Indicators of compromise (IoC) correlation engine

### Behavioral Analysis

Regarding malware and vulnerabilities not tied to signatures, Ermetix provides a component for behavioral analysis of apps and users on a mobile device, composed of a module installed on mobile devices and a behavioral analysis module based on artificial intelligence technologies, for building a model of normal behavior and detecting anomalies with their corresponding risk levels.

The mobile module detects statistical and appropriately anonymized information about mobile device usage. In particular, it provides information about the device's status (temperature, CPU usage, memory usage, battery, etc.) and app usage (system calls, API usage, permissions, and dynamic behavior).

This information is sent in aggregated and anonymous form to the behavioral analysis module, which, using innovative methods based on machine learning and artificial intelligence, creates different models of normal mobile device usage behavior associated with different types of devices/users.

Therefore, based on these models, possible anomalies are detected and sent to the management console along with associated risk levels.

## Key Features of the Module

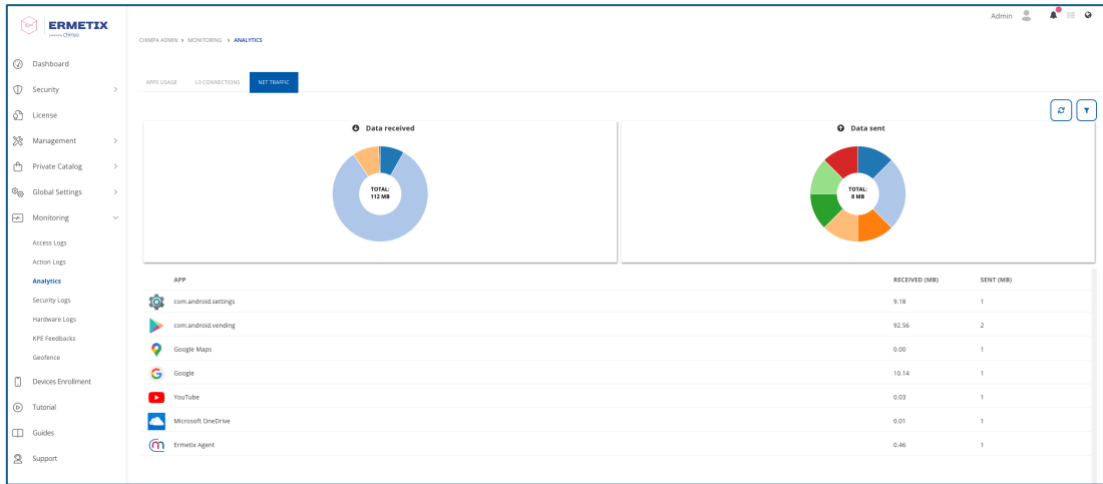
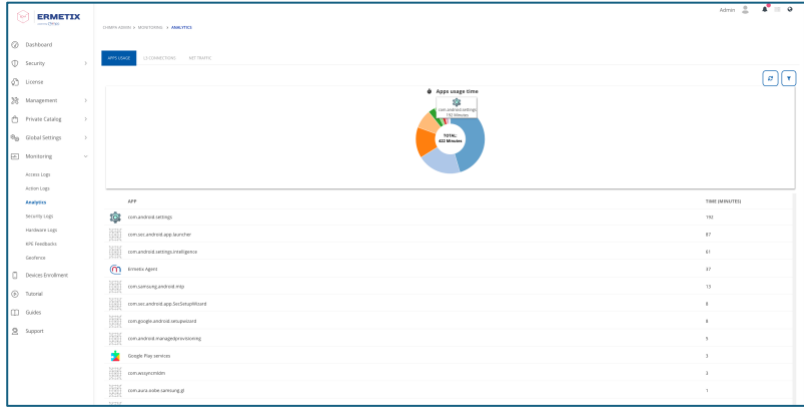
- The machine learning and AI techniques used allow operation even in the presence of heterogeneous data and in the case of missing data (reducing the accuracy of the model only partially).
- Models are built incrementally; if the normal usage profiles of the device change, the algorithm adapts to the change quickly.
- Only statistical and/or appropriately anonymized data are collected to comply with GDPR regulations and not retain sensitive user data.
- Management of different groups and users (group-based policy), to customize mobile device data collection and its display on the management dashboard, ensuring different levels of privacy.

## Logs and Analytical Data

Ermetix allows the collection of various usage logs depending on the operating system installed on the device. Data can be obtained on:

- Connections and domains/IPs contacted
- Volume of incoming/outgoing data divided by domain or IP and application generating the traffic
- Application usage time
- User interactions
- Battery charge/discharge phases
- Security logs from the operating system
- Application permissions
- Failed device unlock attempts
- Monitoring of specific geographical areas (geofencing)
- Hardware usage
- WiFi connections
- RAM usage
- CPU usage
- Others

This data is used by the system to define standard device behaviors and detect any discrepancies in usage. At the same time, some of them (in compliance with privacy regulations) can be viewed from the management panel as shown in the example images below.



**TEMPERATURES**

DEVICE NAME	SERIAL	SENSOR	TEMPERATURE	DATE
Device	R2EN019MCK	Battery	22	18-14-03 14-02-2024
Device	R2EN019MCK	Battery	22	18-14-03 14-02-2024
Device	R2EN019MCK	Battery	22	18-14-03 14-02-2024
Device	R2EN019MCK	Battery	22	18-14-03 14-02-2024
Device	R2EN019MCK	Battery	22	18-14-03 14-02-2024
Device	R2EN019MCK	Battery	21	18-14-03 14-02-2024
Device	R2EN019MCK	Battery	21	18-14-03 14-02-2024
Device	R2EN019MCK	Battery	21	18-14-03 14-02-2024

**RAM**

DEVICE NAME	SERIAL	RAM	DATE
Touchview Gen 5	65W72B-239H90118-00002H	34%	08-16-25 01-02-2024
Touchview Gen 5	65W72B-239H90118-00002H	34%	08-16-25 01-02-2024
Touchview Gen 5	65W72B-239H90118-00002H	34%	08-16-25 01-02-2024
Touchview Gen 5	65W72B-239H90118-00002H	34%	08-16-25 01-02-2024



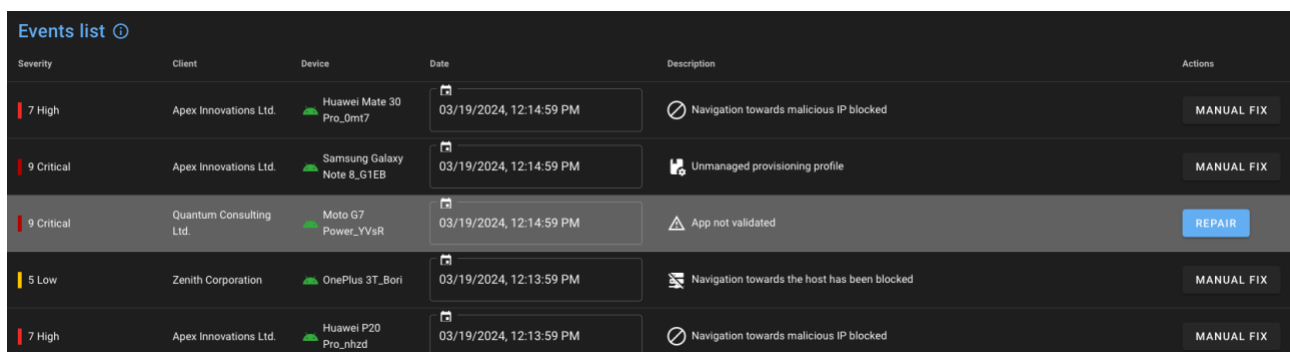
# Passive Security

## Risk Analysis and Non-Conformity Detection

The software analyzes mobile devices to identify potential non-conformities, known vulnerabilities, and provide detailed risk analysis. It identifies vulnerabilities and incorrect configurations that could compromise device security.

Examples of items analyzed include but are not limited to:

- USB debugging enabled
- Installation from unknown sources enabled
- Non-compliant provisioning profiles
- Developer mode enabled
- Passcode (PIN) not enabled or not compliant with established criteria (configurable)
- Jailbreak/root
- Outdated operating system version
- Available updates for the operating system
- Obsolete or updateable applications
- Expired or untrustworthy certificates
- Changes in application permissions
- Device encryption not enabled
- System integrity
- Connections to unprotected WiFi networks
- Obsolete device
- Play Protect status
- CVEs



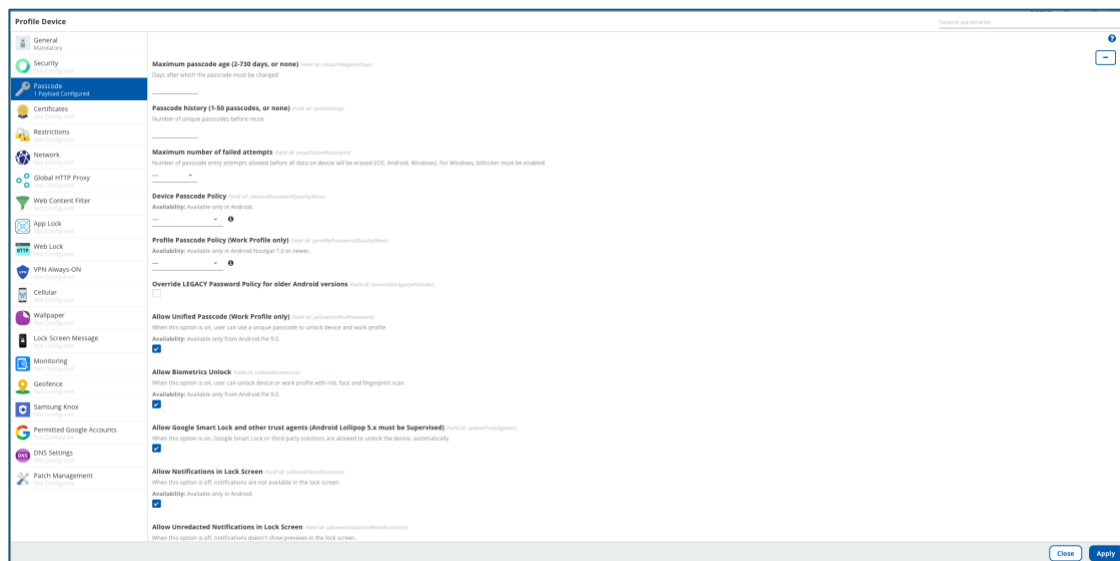
Severity	Client	Device	Date	Description	Actions
7 High	Apex Innovations Ltd.	Huawei Mate 30 Pro_0mt7	03/19/2024, 12:14:59 PM	Navigation towards malicious IP blocked	MANUAL FIX
9 Critical	Apex Innovations Ltd.	Samsung Galaxy Note 8_G1EB	03/19/2024, 12:14:59 PM	Unmanaged provisioning profile	MANUAL FIX
9 Critical	Quantum Consulting Ltd.	Moto G7 Power_VVsR	03/19/2024, 12:14:59 PM	App not validated	REPAIR
5 Low	Zenith Corporation	OnePlus 3T_Bori	03/19/2024, 12:13:59 PM	Navigation towards the host has been blocked	MANUAL FIX
7 High	Apex Innovations Ltd.	Huawei P20 Pro_nhzd	03/19/2024, 12:13:59 PM	Navigation towards malicious IP blocked	MANUAL FIX

In the image, we can see some alerts taken from the Ermetix management console, particularly showing issues related to malware and certificates.

## Fully Configurable Policies

Ermetix provides hundreds of configurations to apply desired policies, including but not limited to:

- Passcode (PIN) criteria
- Certificates to be installed
- Pre-configured WiFi networks
- VPN configuration
- Cellular network configuration
- APN configuration
- System, app, and network restrictions such as
  - Camera usage disablement
  - Airplane mode disablement
  - USB debugging and/or unknown sources disablement
  - Allow-list/Block-list of APPs
  - Cloud backup usage disablement
  - Incoming/outgoing call disablement
  - Minimum WiFi security level



In the image, a configuration profile for Android devices is visible.

## Data Analysis and Attack Prevention

Ermetix analyzes information to prevent various types of attacks and increase security, such as:

- Through certificate analysis, reducing the likelihood of MITM attacks

- Analyzing domain resolution and connections to limit attacks like ARP poisoning or SSL stripping
- Observing data volume received/sent over time to work on SQL injection attacks
- Studying general device usage through behavioral analysis to prevent other attacks, following the Mitre Att&ck matrices
- Disconnecting or reporting insecure networks that do not meet imposed security policies

## Ermetix Web Console

### Console Notifications

The administration console allows users to view, search, and filter the results of all scans, providing administrators with maximum control over device security.

In the image above, the list of periodic scans performed on devices is visible. Clicking on a single row allows viewing the scan details as indicated by the arrow.

In the image below, we see an alert related to automatically removed malware.

The dashboard is also updated in real-time through the "operations" tab, allowing users to view security notifications as soon as events are recorded.

### Automatic and/or Manual Remediation

It is possible to configure remediation actions that will be automatically applied when certain events occur or choose to intervene manually. Automatic remediation actions available include:

- Device initialization
- Emergency mode activation
- OS update
- App update
- App removal
- Passcode (PIN) setting
- Lost mode activation
- WiFi disconnection
- Bluetooth disablement
- Blocking of unsafe domains/IPs
- VPN configuration and enablement
- Hardware disablement/enablement (such as GPS, Bluetooth, hotspot)
- Network traffic blocking (sinkhole)

## Advanced and Dynamic Filters

All charts in the console allow users to filter displayed data with a single click based on dates, locations, event types, operating system, and event severity.

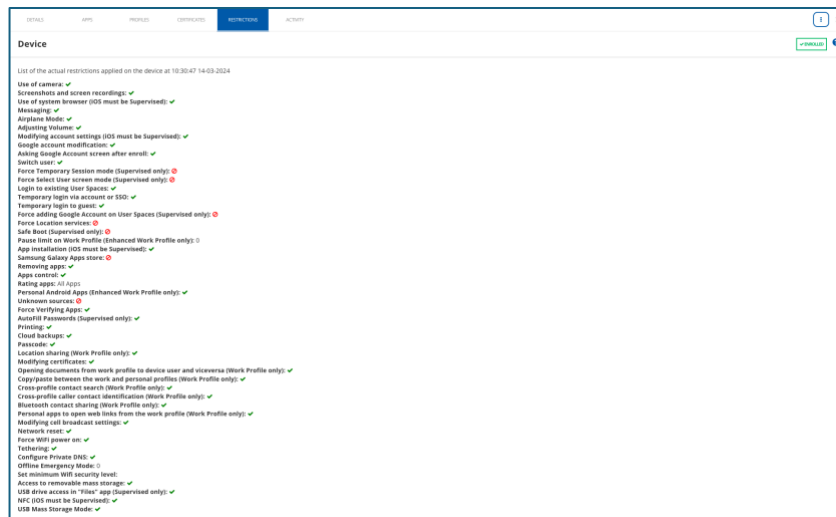
## Device Inventory

From the management console, users can view the list of devices, with each device having details about security posture, hardening actions to be taken, and other significant data including:

- Identifiers: Serial, MAC address, Manufacturer, ID.
- Operating System: Type, Version, Build.
- Specifications: Storage, CPU, GPS, RAM, Resolution.
- Security: Root, encryption, passcode, location, lost mode, antivirus.
- Agent Version
- Network: Public IP address, Local IP address, WiFi status, WiFi SSID, VPN.
- Available updates
- Groups: Configured groups.
- Security status: Anti-malware scan results, firewall rules, website blocklists.
- Applications: List of installed applications with available updates.

Among the device security risk configurations, you can also view, among others:

- USB debugging status;
- Application installation permission;
- Installation of apps from unknown sources;
- Developer mode;
- Passcode status;
- Encryption status;
- Root status;
- Software information.



In the image above, we can see how the management console displays the main restrictions applied (or not) on a device.

By analyzing data such as restrictions, security alerts, scan results, and log monitoring, Ermetix can provide a security score for each device that is viewable in dedicated sections of the management panel.

This value is expressed on a scale from 0 to 10 (thus comparable to the standard risk assessment system adopted by NIST) and allows users to quickly identify the current situation regarding device security.

## Group-based Device Management

One of Ermetix's key features is the ability to configure different operating groups, allowing administrators to organize and manage devices more efficiently.

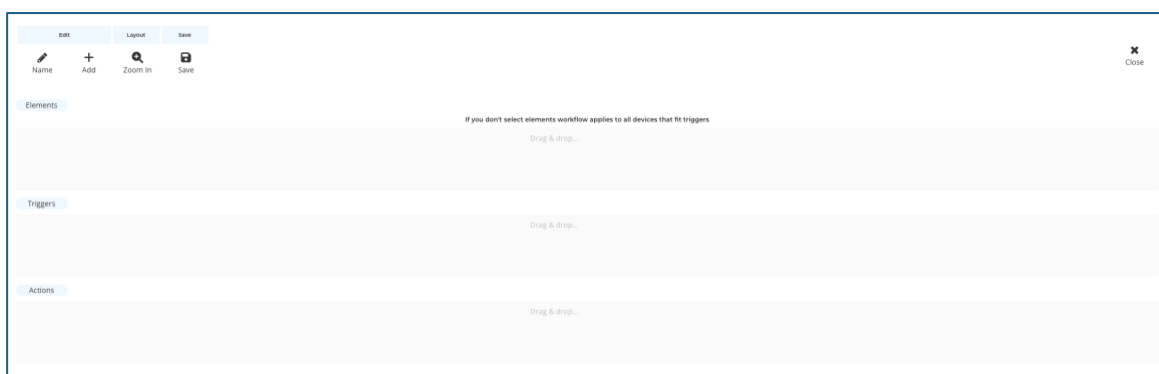
Within the administration panel, users can access detailed information about each device, including the operating groups they belong to. This allows users to have a clear view of device configuration and assignment to various groups.

In particular, Ermetix allows comprehensive and modular device management through groups, tags, or "smart workflows".

The data available on the administration console and hardening policies can be easily managed from the management console on multiple devices simultaneously through custom groups. Additionally, it's possible to create groups that will be dynamically filled based on certain conditions defined by the console user.

Examples:

- Manually creating device groups on the management panel
- Creating a "smart workflow" that adds one or more devices to a "dynamic" group when certain conditions occur
- For each group, specifying different policies



In the image above, it is shown how it is possible to dynamically add a device to a group.

It's worth noting the possibility of exporting and importing all group profiles in JSON format.

## Data Visualization Based on Permissions

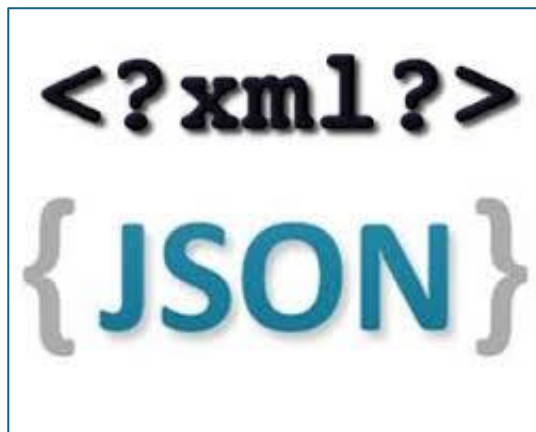
The management console offers some preset roles such as the administrator role, while also offering the ability to configure customizable roles by assembling permission groups. This is essential for ensuring access at different levels to available data.

Based on permissions, it is also possible to configure alerts and console sections to show to the logged-in user. An example is provided in the image below.

## Exporting Data from the Management Console

Security data of devices present in the management console can be exported in various ways. In particular, it is possible to:

- Export to other services via JSON or XML
- Export data as PDF or CSV directly from the panel
- Export raw syslog to .log files
- Utilize integration with third-party services (SIEM) with syslog data in a format compatible with international standards.



## Ermetix Agent on Mobile Devices

The installation procedure of the Ermetix Agent on Android and iOS is simplified. It's possible to start the configuration in a zero-touch manner by scanning a QR code or by downloading the app directly from the App Store and Play Store.

## Device Notifications

Notifications regarding scans are also available on mobile devices to keep the end-user constantly informed. Two types of notifications can be configured for the user:

- **Popup Notifications:** These are displayed directly on the user's screen to immediately draw their attention. These notifications inform the user about important updates regarding periodic and real-time antivirus scans. They indicate the start of a scan, successful completion of a scan, and detection of any threats.
- **Alerts Section Notifications:** These are displayed within the dedicated alerts section of the antivirus user interface. These notifications provide a detailed log of antivirus events, allowing the user to access information at any time. Through this section, the user can review scan history, check which threats have been detected, and obtain details on any issues encountered.

Thanks to the combined use of popup notifications and alerts section notifications, the system ensures effective and timely communication between the user and the administrator, keeping them constantly informed about events and allowing them to promptly take necessary measures to ensure system security.

These notifications are pre-configured and automatic; however, it is possible to configure custom notifications to be sent to the device directly from the administration console.

## Emergency Mode

Emergency mode is automatically initiated following the detection of threats or risks that cannot be automatically remediated. This allows containing malware/threats without them being able to access or compromise sensitive data and apps.

The activation of emergency mode can be configured directly on Ermetix in the following cases:

- Malware or threats that cannot be automatically removed or remediated;
- The device is isolated from the Ermetix server for a defined period;
- Permissions required for device monitoring and protection are tampered with or revoked;
- Compliance rules are not met.

## Sharing Data on the Device

In order to provide a comprehensive overview of antivirus behavior and scans, the Chimpa Agent will send a specific broadcast message at the end of each scan containing details of the files and apps analyzed via JSON format.

Below are the details of the Intent sent in broadcast for Android devices:

Action: eu.chimpa.mdmagent.ANTIMALWARE\_SCAN;  
Extras: "info";

JSON structure of the "info" extra:

```
public class ScanJson {  
  
    @Json(name = "scanId")  
    public Long scanId;  
  
    @Json(name = "timestamp")  
    public Instant timestamp;  
  
    2 usages  
    @Json(name = "malwares")  
    public List<MalwareJson> malwareJsonList;  
  
    @Json(name = "fileCount")  
    public Long fileCount;  
  
    @Json(name = "periodic")  
    public Boolean periodic;  
}
```

```
public class ScanJson {  
  
    @Json(name = "scanId")  
    public Long scanId;  
  
    @Json(name = "timestamp")  
    public Instant timestamp;  
  
    2 usages  
    @Json(name = "malwares")  
    public List<MalwareJson> malwareJsonList;  
  
    @Json(name = "fileCount")  
    public Long fileCount;  
  
    @Json(name = "periodic")  
    public Boolean periodic;  
}
```

## Additional Features

### Sending Actions to the Device

Through the web panel, it is possible to send some actions directly to one or more devices. For the action to be received, the device must be connected to the network.



Security-related actions include: Set/reset Lock Code, screen lock, Factory Data Reset Protection, Enable lost mode.

**Setting/resetting Lock Code:** These actions allow the administrator to remotely set a PIN on the individual device or remove it to access the device if the lock code is forgotten.

**Screen lock:** This action locks the screen if the device's screen is on. If the device has a configured lock code, it will be immediately requested to unlock it.

**Enable Factory Data Reset Protection (Android):** This action, available only for Android, requires specifying a Google account. This Google account will be required to unlock the device after a factory reset. The Google account will also be required if the device is reset via Hard Reset.

**Enable lost mode :** This action sets a lock PIN and enables lost mode on the device . Contact information is displayed on the lock screen. Upon unlocking the phone, the exact location of the device is sent, which can be viewed on the web panel.

## Actions related to apps & media: install or remove apps/APKs, upload or delete files.

With these actions, you can select an app from the relevant store (Play Store for Android, App Store for iOS) and send the installation command for it.

Additionally, for Android, you can install an APK by providing a direct link to the .apk file that can reside on Dropbox, Google Drive, or OneDrive.

Note: To successfully install the APK, it is necessary to enable the "Allow unknown sources" option in Restrictions.

## Device-related actions: notification, reboot, shutdown, initialize.

**Notification:** This action sends a message to the device, which can be a full-screen popup or a simple notification with a text message.

**Initialize:** This action sends a factory reset command to the device. Note: This action disconnects the device from remote control and must be re-registered.

## Installation of Configuration Profiles

With configuration profiles, it is possible to remotely calibrate the behavior of devices and the functions accessible to users who use them.

For example, you can apply Restrictions such as setting a list of unusable apps, blocking the camera, inhibiting screenshots, preventing factory reset.

You can also send a set of saved Networks that are stored on the device and set that the device can only connect to these and not to other available networks.

Through these profiles, you can enable Kiosk Mode through App Lock, which limits the use of only certain applications on the device, or Web Lock, which locks the device to a browser by opening a defined link. Profiles can also act on all aspects related to the device such as Allowed Google Accounts, Geofencing, Background Management, and screen lock security code policy.

## Screen Lock Code Policy

This feature sets the minimum security policy that must be met on the device. For example, a Low policy allows a 4-character numeric PIN to be sufficient on the device, while a High policy requires an alphanumeric password to disable the screen lock.

If the minimum policy is not met, the device will go into Emergency Mode, which will only be disabled by entering the required screen lock code.

## Device Hardening

Ermetix provides over 200 possible restrictions that regulate device usage and block or limit the features accessible to the user in order to maintain passive control over the device.

In the image above, we can observe the macro-areas in which the applicable restrictions are divided.

Some of the available restrictions include:

**System:** inhibit factory data reset and account addition. These two options disable the possibility for the user using the device to reset it to factory data and to add accounts.

By enabling these settings, the device cannot exit remote control and policies set via the web panel by initializing the device manually, nor can applications be installed through app stores via the user's personal account.

**System:** inhibit developer mode. Developer mode on the device is blocked through restrictions. This mode, if activated, allows the user to compromise the device's integrity. Through applied restrictions, this functionality is denied by default.

**App & content:** allowlist/blocklist App. In this section, you can define an Allowlist, a list of allowed apps that are the only ones that can be used, or a Blocklist, a list of apps that, even if installed, are hidden and cannot be used.

**Network & cellular:** force access only to configured WiFi. With this option, the device's connection is limited only to WiFi networks configured in the same profile. To enable this

option, it is necessary to specify at least one SSID and password in the saved Networks to which the device can connect.

This option, when set, allows verifying the minimum security level of the WiFi password to which the device connects.

For example, you can exclude WiFi networks that use WEP or WPA encryption and allow only WiFi networks that use WPA2 encryption.

**Saved Networks:**

You can define Saved Networks by specifying SSID and Password. The networks defined here will be saved on the device, allowing it to connect without manually entering the password.

**Web Content Filtering:**

You can define a list of websites that the device's system browser cannot access (Blocklist) or a limited list that it can access, excluding all others (Allowlist).

**App Lock/Web Lock Functionality:**

These features enable kiosk mode on the device, limiting its usage to a specified list of applications.

Typically, this mode is used for devices like advertising kiosks, terminals with general information, but also for tablets used for restaurant orders, public service tablets, etc.

With the App Lock feature, you define a list of applications to be used. Once defined, the device enters kiosk mode and only the specified apps can be opened. The device remains in this state until the profile is removed.

The Web Lock feature works similarly, except that you specify a URL.

**Geofencing:**

This feature communicates to the device the geofenced areas for control. Enabling these areas allows various functionalities, such as receiving an email notification when the device enters or exits the area or enabling certain configurations only when the device is in these areas.

**Request Location:**

You can request the device's location from the web panel. The location will then be displayed on the panel in the device details tab. This feature can be useful for identifying the device's location with a reasonable degree of accuracy, calculated by triangulating the position obtained through IP network and GPS.

**External Device Blocking:**

Ermetix allows total control over both physical and device connections, data from external mass storage (USB mass storage, SD card, etc.), or proximity connections like Bluetooth and NFC. You can configure this feature to prevent such accesses from becoming vectors for potential malware infections or to prevent exfiltration of critical data from targeted devices.