ERMETIX

Datasheet

Ver.1.3

Sommario

Sommario 1
Panoramica del prodotto: 3
Funzionalità principali 3
Sicurezza 4
Sicurezza attiva 4
Protezione in tempo reale 4
Scansioni periodiche 4
Nell'immagine è possibile vedere il riepilogo degli avvisi relativi alle scansioni sul dispositivo 5
Modalità offline 5
Safe browsing 6
Threat intelligence 7
Analisi comportamentale 7
Log e dati analitici 7
Sicurezza Passiva 8
Analisi del Rischio e Rilevamento delle Non-conformità 8
Politiche completamente configurabili 9
Analisi dei dati e prevenzione attacchi 10
Ermetix Web Console 12
Notifiche sulla console 12
Remediation automatica e/o manuale 13
Filtri avanzati e dinamici 14
Censimento dei dispositivi 14
Gestione dei dispositivi basata su gruppi 15
Visualizzazione dei dati basata su permessi 17
Esportazione dei dati dalla console di gestione 18
Ermetix Agent sui dispositivi mobili 19
Notifiche sul dispositivo 19
Modalità Emergenza 20
Condivisione dei dati sul dispositivo 21
Funzionalità aggiuntive 22
Invio di azioni al dispositivo 22
Azioni relative alla sicurezza: Imposta/resetta Codice di sblocco, blocca schermo, Protezione Ripristino dati fabbrica, Abilita modalità smarrito 22
Imposta/resetta Codice di sblocco 22
Blocca schermo 22
Abilita Protezione Ripristino Dati di Fabbrica (Android) 22
Abilita modalità smarrito (iOS) 22
Azioni relative a apps & media: installa o rimuovi app/apk, carica o elimina file 23
Azioni relative al dispositivo: notifica, riavvia, spegni, inizializza 23
Installazione dei profili di configurazione 24
Policy Codice Blocca Schermo 24
Hardening 25

Panoramica del prodotto:

Ermetix è una potente soluzione software progettata per fornire un quadro completo del censimento dei dispositivi mobili **(Android, iOS, iPadOS, tvOS) oltre che di dispositivi Windows 10 ed 11** e della loro postura di sicurezza.

Con una dashboard intuitiva e ricca di funzionalità, **Ermetix** consente di visualizzare grafici e statistiche filtrabili e dinamiche.

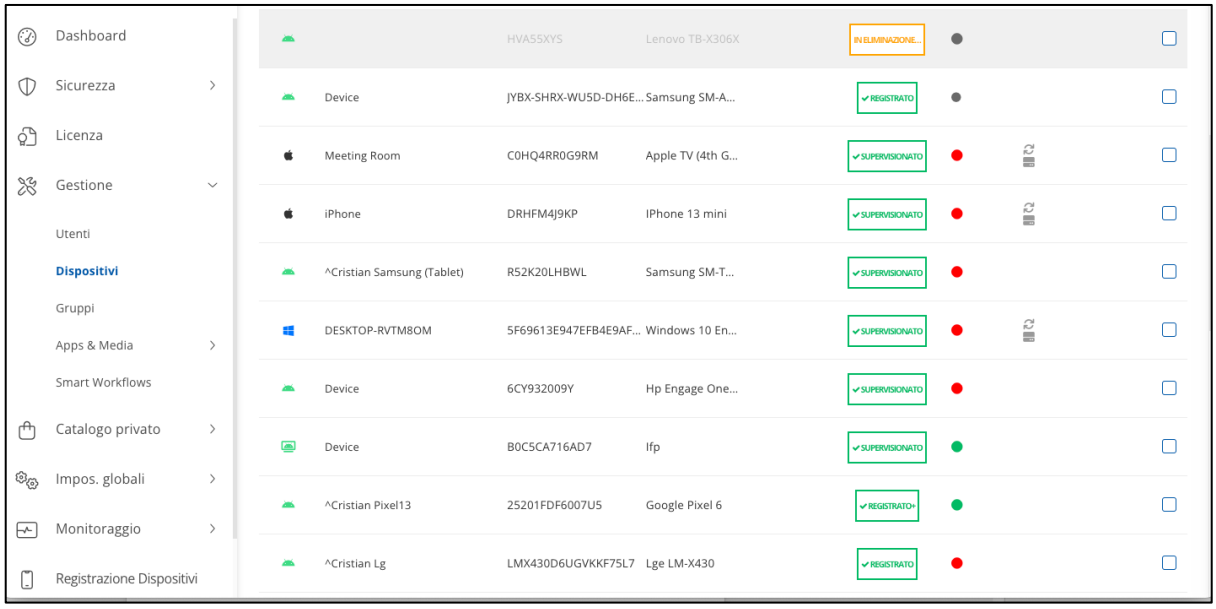
Il software fornisce inoltre una lista dettagliata degli **eventi di sicurezza** rilevati sui vari dispositivi, consentendo un'analisi approfondita delle minacce e delle vulnerabilità.

Funzionalità principali

Ermetix è una piattaforma che permette di monitorare, proteggere e gestire il proprio parco dispositivi tramite una console web.

Previa configurazione semplice e intuitiva, Ermetix è in grado di monitorare e proteggere i dispositivi lavorando su tre diversi livelli di sicurezza:

- **attiva** (scansioni anti-malware periodiche, protezione anti-malware real-time e navigazione sicura)
- **threat intelligence** (analisi comportamentale e correlazione degli IOC)
- **passiva** (hardening delle impostazioni critiche, vulnerabilità note, configurazione regole di compliancy, patch management)



Sicurezza

Sicurezza attiva

Protezione in tempo reale

Ermetix permette di monitorare in tempo reale i dispositivi analizzando potenziali **malware** ogni qualvolta sia necessario; in particolare sono previste scansioni quando:

- un file viene scaricato/creato, modificato o spostato
- una cartella viene creata, modificata o spostata
- un'app viene installata

Scansioni periodiche

Le **scansioni periodiche,** invece, vengono avviate ogni 24 ore a partire dalla prima configurazione dell'anti-malware. Questo tipo di scansione copre l'intero file system e le applicazioni installate ed è utile per individuare i **malware dormienti** e gli eventuali malware presenti nel firmware del dispositivo.

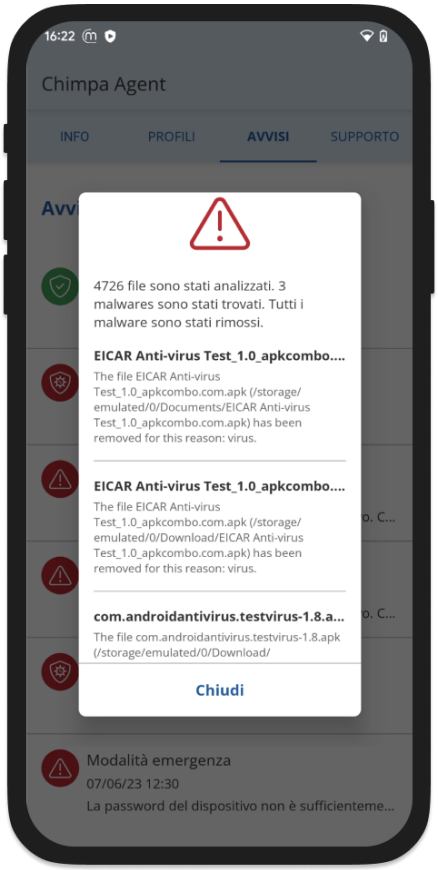
Dettagli sulle scansioni:

Le scansioni effettuate da **Ermetix** avvengono tramite le applicazioni specifiche per ogni sistema operativo che

- monitorano i cambiamenti di tutti i file del f**ile system** e avviano una scansione ad hoc ogni volta che un file viene aggiunto, modificato o spostato, garantendo la sicurezza del dispositivo in ogni momento.
- **scansionano ricorsivamente** tutte le cartelle interessate dalla modifica al punto sopra
- analizzano ogni app non appena viene installata e la disinstallano nel caso in cui risulti positiva ad una scansione anti-malware.

Questi tipi di scansioni sono basati su firme che vengono aggiornate periodicamente; questa componente del sistema, quindi, lavora su malware noti.

L'aggiornamento delle firme avviene con **metodo push** da Ermetix al dispositivo.



Nell'immagine è possibile vedere il riepilogo degli avvisi relativi alle scansioni sul dispositivo

Modalità offline

I dispositivi vengono monitorati anche quando sono **offline** grazie alle firme presenti sul dispositivo stesso e agli algoritmi eseguiti per cercare potenziali malware senza firma nota. Questa caratteristica è particolarmente utile in situazioni in cui il dispositivo non può accedere alla rete, ad esempio in luoghi dove la linea internet è assente o carente.

Nel caso il dispositivo sia offline ovviamente non potrà comunicare i dati relativi alle scansioni alla console di amministrazione; tali dati verranno, comunque, inviati a Ermetix al **primo momento utile.**

Per tutte le rilevazioni il sistema rimedia automaticamente e qualora non fosse possibile applicare una **remediation automatica** è possibile attivare la **modalità emergenza** (configurazione disponibile dalla console di gestione).

E' da notare che la prima configurazione richiede una connessione internet per poter permettere al dispositivo di scaricare i dati necessari alla svolgimento delle successive scansioni così come è **necessaria una connessione** per poter scaricare gli aggiornamenti delle firme.

Safe browsing

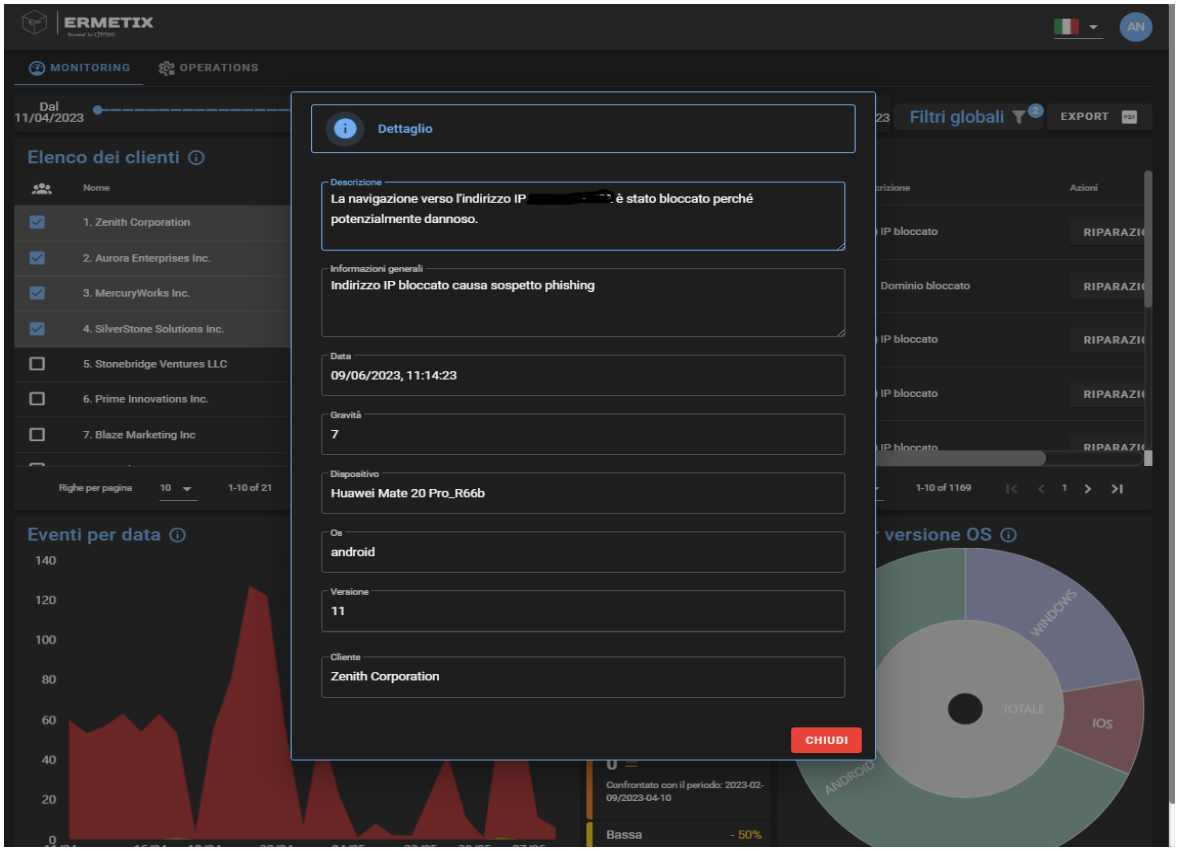
Ermetix permette agli utenti di navigare in modo sicuro; grazie alla protezione del **Safe Browsing**, infatti, è possibile prevenire in primis che l'utente visiti **siti web potenzialmente dannosi** e, in secondo luogo, che applicazioni potenzialmente **malevole** contattino IP/domini malevoli.

Questa funzionalità è, inoltre, utile nel caso in cui il dispositivo non sia compliant con le policy di sicurezza: in questo caso, infatti, **Ermetix** può scartare tutti i pacchetti del traffico di rete (**sinkhole**).

Chi visualizza la console di gestione può verificare tutte le risorse che vengono bloccate sui dispositivi oltre che bloccare/permettere la navigazione verso IP/domini preimpostati attraverso meccanismi di **allow-list e block-list.**

Ermetix offre, inoltre, la possibilità di utilizzare **DNS sicuri** per la risoluzione dei domini.

Nell'immagine sottostante possiamo vedere come sul pannello di Ermetix si possano individuare facilmente gli indirizzi bloccati dal sistema di Safe browsing, in questo caso particolare è stato bloccata la navigazione verso un IP riconducibile ad attività di phishing



Threat intelligence

Analisi comportamentale

Riguardo l'analisi di malware e vulnerabilità non vincolate a firme Ermetix fornisce un componente per l'analisi comportamentale relativo alle app e agli utenti di un dispositivo mobile, composta da un **modulo** che si **installa sui dispositivi mobil**i e un **modulo di analisi comportamentale** basato su tecnologie di intelligenza artificiale, per la costruzione di un modello di comportamento normale e il rilevamento di anomalie con relativo livello di rischio.

Il modulo mobile, che rileva informazioni statistiche e opportunamente anonimizzate sull'uso del dispositivo mobile. In particolare, **fornirà informazioni sullo stato del dispositivo** (temperatura, uso CPU, utilizzo memoria, batteria, ecc.) e sull'utilizzo delle app (system call, uso di API, permessi, e comportamento dinamico).

Tali informazioni saranno inviate in forma aggregata e anonima al modulo di analisi comportamentale che, tramite **metodi innovativi** basati sul **machine learning** e sull'intelligenza artificiale permette di creare diversi modelli di comportamento normale di uso del dispositivo mobile associati a diversi tipi di dispositivi/utente.
Quindi, basandosi su tali modelli, saranno rilevate e inviate alla console di gestione le possibili anomalie con associati i livelli di rischio.

Feature principali del modulo:

- Le tecniche di **machine learning e AI** utilizzate permettono di operare anche in presenza di dati non omogenei e nel caso di dati mancanti (riducendo solo in parte l'accuratezza del modello).
- I modelli sono costruiti in maniera incrementale; se cambiano i profili normali di uso del dispositivo, l'**algoritmo si adatta in breve tempo al cambiamento.**
- Sono raccolti solo dati statistici e/o opportunamente anonimizzati in modo da rispettare le **normative GDPR** e non conservare dati sensibili dell'utente.
- Gestione di gruppi e utenti differenti (group based policy), in modo da personalizzare la raccolta di dati sul dispositivo mobile e la relativa visualizzazione sulla dashboard di gestione, in modo da garantire diversi livelli di privacy.

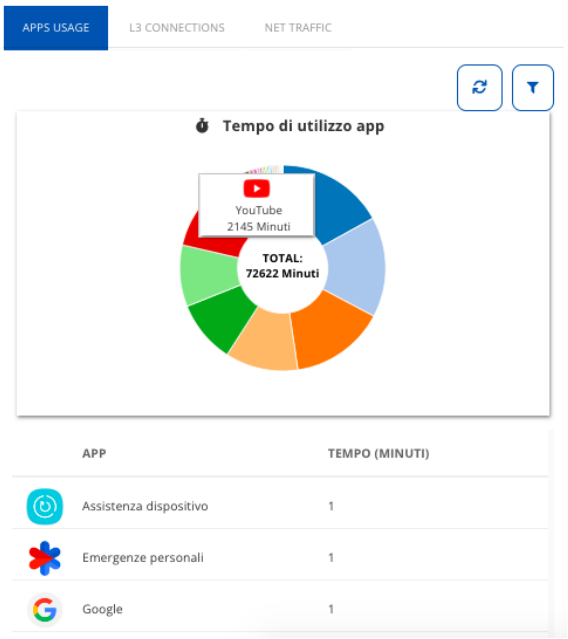
Log e dati analitici

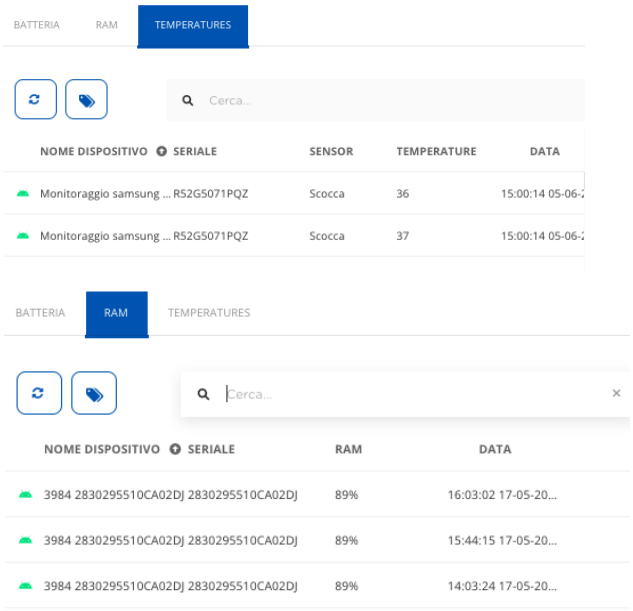
Ermetix consente di collezionare diversi log di utilizzo a seconda del sistema operativo installato sul dispositivo possono essere ricavati dati su:

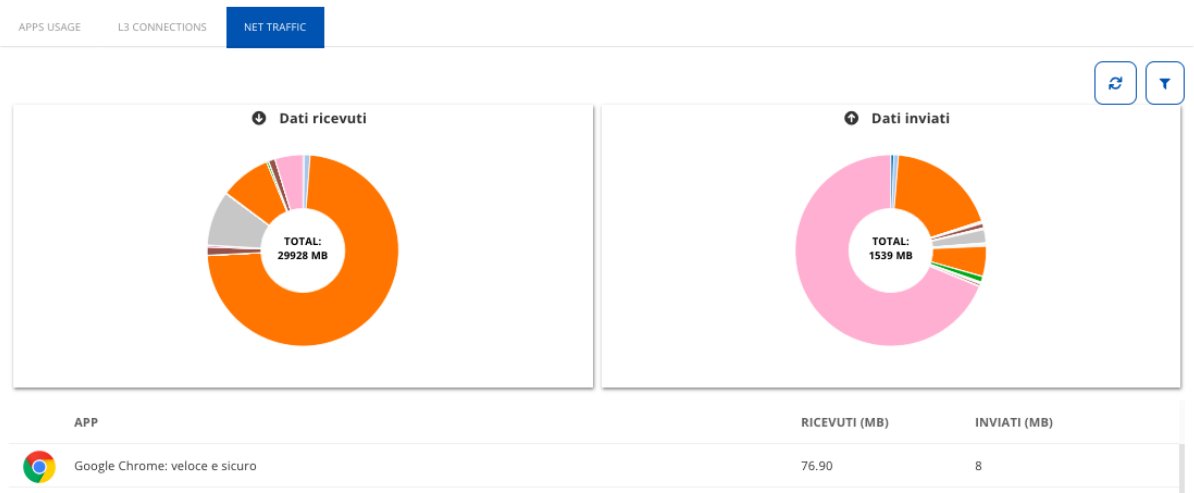
- connessioni e domini/IP contattati
- mole di dati in ingresso/uscita divisi dominio o IP e applicazione che genera il traffico
- tempo di utilizzo delle applicazioni
- interazioni utente
- fasi di carica/scarica della batteria

- log di sicurezza derivanti dal sistema operativo
- permessi delle applicazioni
- tentativi di sblocco del dispositivo falliti
- monitoraggio di specifiche aree geografiche (geofence)
- utilizzo hardware
- connessioni WiFi
- utilizzo RAM
- utilizzo CPU
- altro

Questi dati vengono utilizzati dal sistema per definire i comportamenti standard del dispositivo e rilevare eventuali discrepanze di utilizzo, al tempo stesso alcuni di essi (nel rispetto della normativa privacy) sono visualizzabili dal pannello di gestione come mostrato nelle immagini di esempio sottostanti.







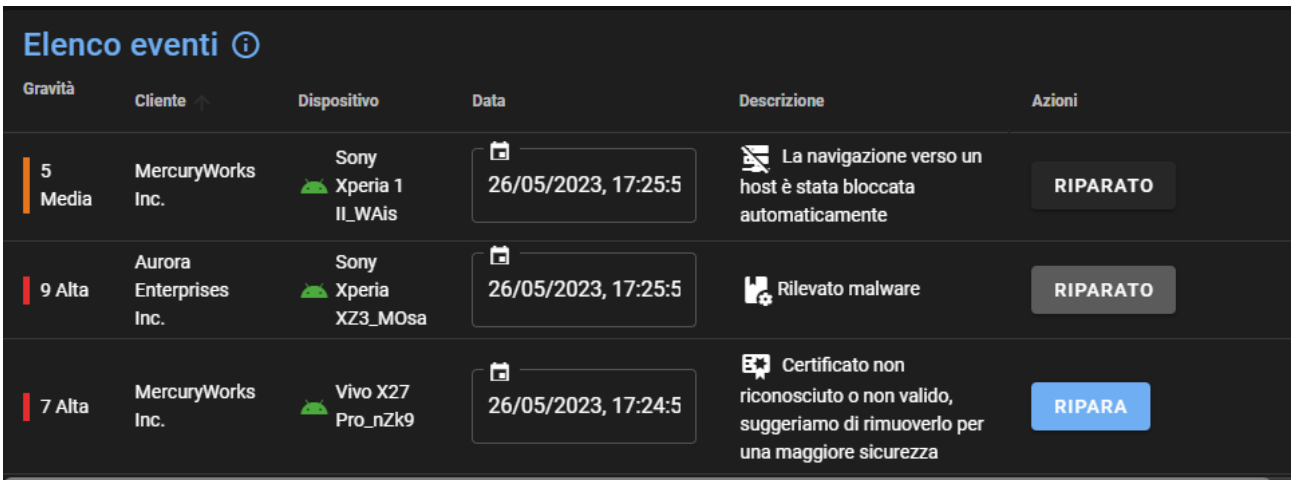
Sicurezza Passiva

Analisi del Rischio e Rilevamento delle Non-conformità

Il software analizza i dispositivi mobili per individuare potenziali non-conformità, vulnerabilità note e fornire un'analisi del rischio dettagliata. Identifica vulnerabilità e configurazioni errate che potrebbero mettere a rischio la sicurezza dei dispositivi.

Vengono analizzati a titolo esemplificativo e non esaustivo:

- Debug USB abilitato
- Installazione da sorgenti sconosciute abilitata
- Profili di provisioning non conformi
- Modalità sviluppatore abilitata
- Passcode (PIN) non abilitato o non conforme ai criteri stabiliti (configurabili)
- Jailbreak/root
- Versione del sistema operativo obsoleta
- Aggiornamento disponibile per il sistema operativi
- Applicazioni obsolete o aggiornabili
- Certificati scaduti o non attendibili
- Cambiamenti nei permessi delle applicazioni
- Encryption del dispositivo non abilitata
- Integrità di sistema
- Connessioni a reti WiFi non protette
- Dispositivo obsoleto
- Stato del Play Protect
- CVE

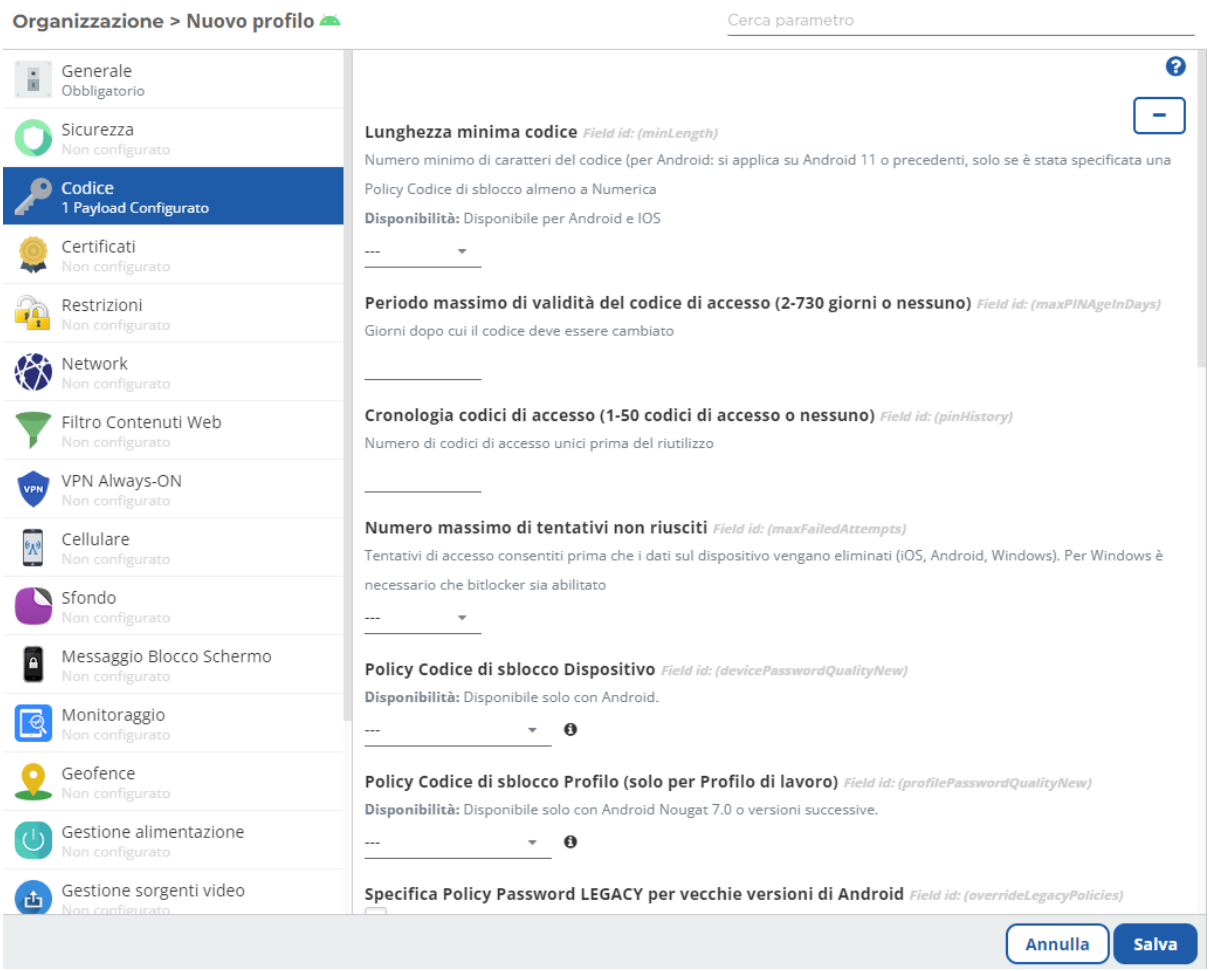


Nell'immagine possiamo vedere alcuni avvisi presi dalla console di gestione di Ermetix, in particolare vediamo come sia possibile visualizzare problematiche su malware e certificati.

Politiche completamente configurabili

Ermetix mette a disposizione centinaia di configurazioni per poter applicare le politiche desiderate, a titolo esemplificativo e non esaustivo:

- Criteri per il passcode (PIN)
- Certificati da installare
- Reti WiFi da pre-configurare
- Configurazione VPN
- Configurazione rete cellulare
- Configurazione APN
- Restrizioni di sistema, app, rete come
    - Disabilitazione utilizzo della fotocamera
    - Disabilitazione utilizzo modalità aereo
    - Disabilitazione utilizzo debug USB e/o sorgenti sconosciute
    - Allow-list/Block-list di applicazioni
    - Disabilitazione di utilizzo backup su Cloud
    - Disabilitazione chiamate in entrata/uscita
    - Livello minimo di sicurezza WiFi



Nell'immagine è visibile un profilo di configurazione per dispositivi android

Analisi dei dati e prevenzione attacchi

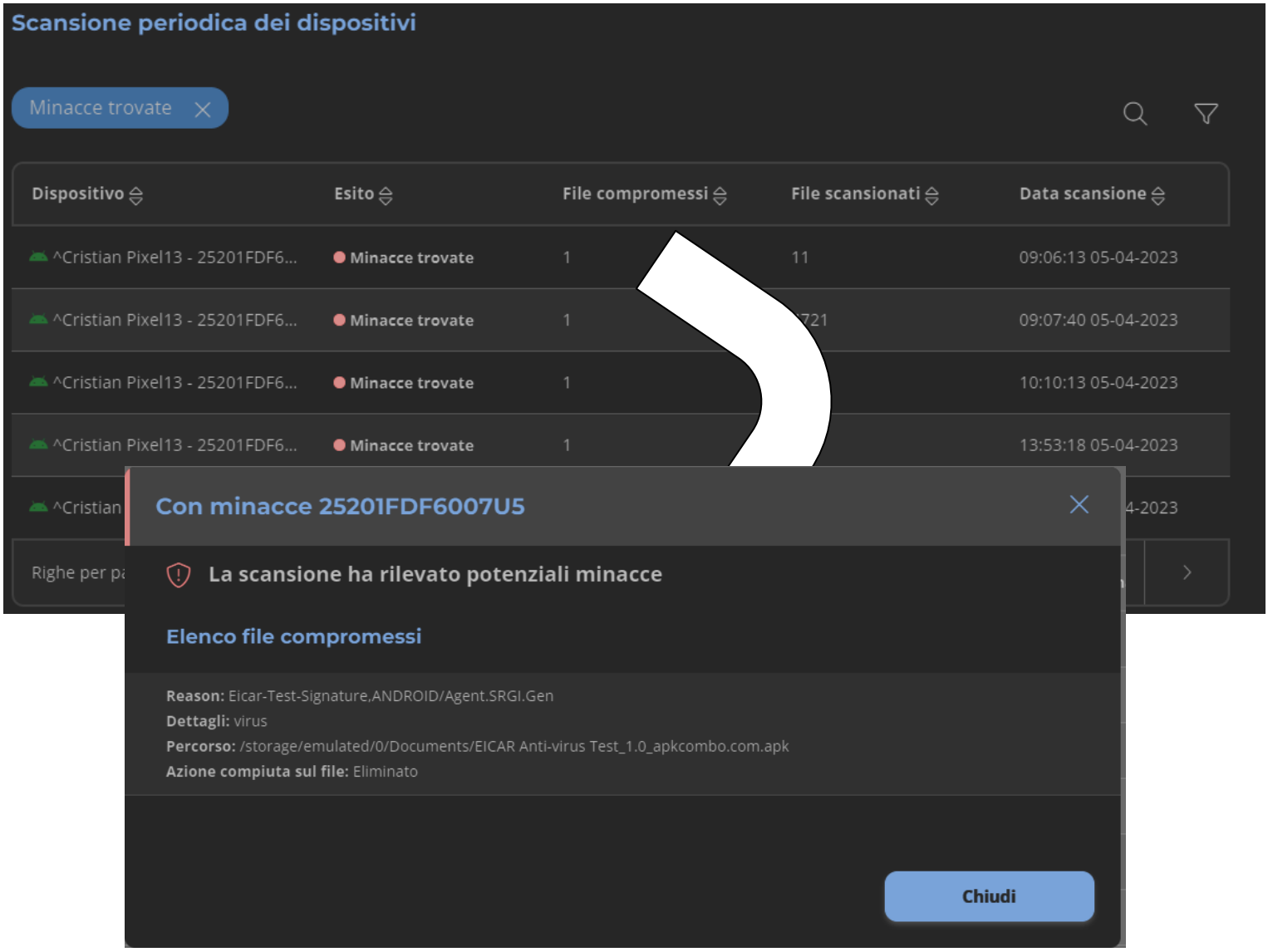
Grazie alle informazioni analizzate da Ermetix è possibile prevenire molteplici tipi di attacchi ed aumentare la sicurezza, per esempio:

- tramite l'analisi dei certificati è possibile attenuare le probabilità di attacchi MITM
- lo studio della risoluzione dei domini e delle connessioni permette di limitare attacchi come ARP poisoning o SSL stripping
- l'osservazione della mole di dati ricevuti/inviati nel tempo permette di lavorare sugli attacchi di SQL injection
- studiando l'utilizzo generale del dispositivo mediante analisi comportamentale è possibile prevenire altri attacchi, anche seguendo le matrici del Mitre Att&ck
- disconnettere o segnalare le reti poco sicure o che non soddisfano le politiche di sicurezza imposte

Ermetix Web Console

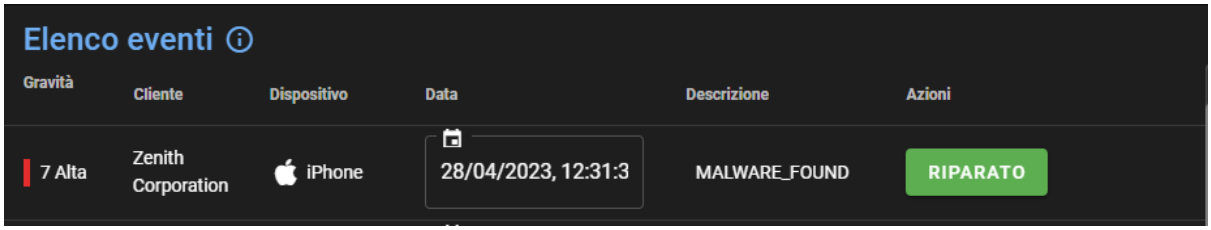
Notifiche sulla console

Sulla console di amministrazione è possibile visualizzare, cercare e filtrare i risultati di tutte le scansioni effettuate consentendo all'amministratore di avere il massimo controllo sulla sicurezza dei dispositivi.

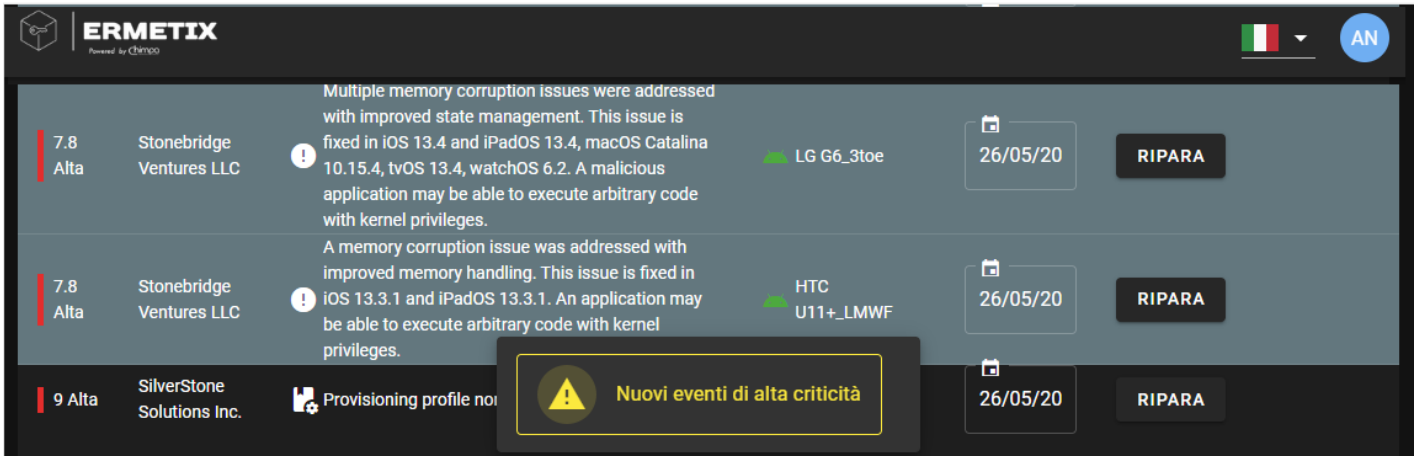


Nell'immagine sopra è possibile visualizzare la lista delle scansioni periodiche effettuate sui dispositivi. Al click sulla singola riga è possibile visualizzare il dettaglio della scansione come indicato dalla freccia.

Nell'immagine sottostante vediamo un avviso relativo a malware automaticamente rimosso



La dashboard, inoltre, viene aggiornata in tempo reale grazie al "tab operations" che permette di visualizzare le notifiche di sicurezza non appena gli eventi vengono registrati



Dettaglio del tab "operations" della console web, qui vengono riportati gli avvisi in tempo reale

Remediation automatica e/o manuale

E' possibile configurare le azioni di remediation che verranno applicate automaticamente al verificarsi di determinati eventi oppure è possibile scegliere di intervenire manualmente, in particolare le azioni di remediation automatiche a disposizione sono:

- Inizializzazione del dispositivo
- Abilitazione modalità emergenza
- Aggiornamento os
- Aggiornamento app
- Rimozione app
- Impostazione passcode (PIN)
- Attivazione modalità smarrito
- Disconnessione da WiFi
- Disabilitazione del Bluetooth
- Blocco di domini/IP considerati non sicuri
- Configurazione e abilitazione VPN
- Disabilitazione/abilitazione hardware (quali GPS, Bluetooth, hotspot)
- Blocco del traffico di rete (sinkhole)

Filtri avanzati e dinamici

Tutti i grafici presenti nella console permettono, con un singolo click, di filtrare i dati visualizzati basandosi su date, sedi, tipologia di evento, sistema operativo e gravità dell'evento.

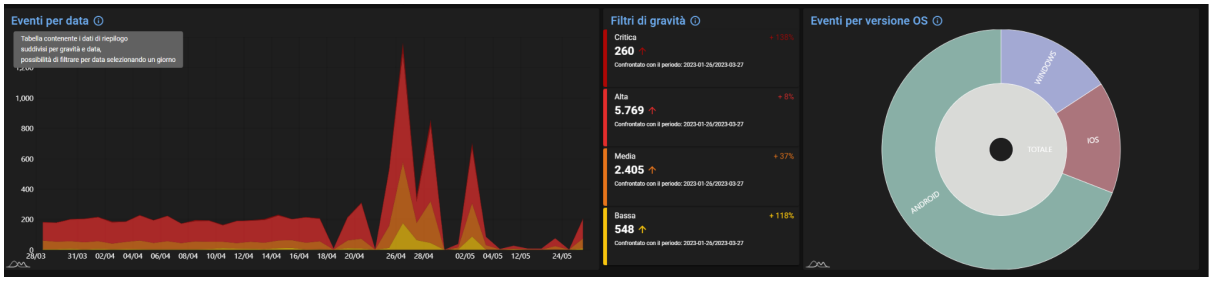


Immagine dei grafici filtrabili presenti nel tab "monitoring" della console di gestione

Censimento dei dispositivi

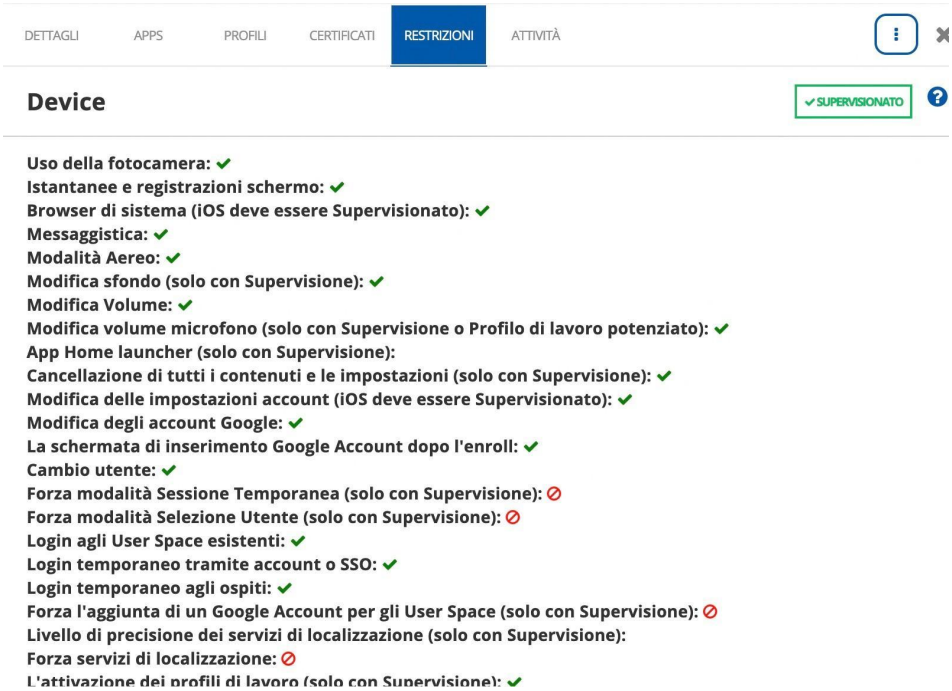
Dalla console di gestione è possibile visualizzare la lista dei dispositivi, per ogni dispositivo sono previsti dettagli sulla postura di sicurezza, azioni di hardening da intraprendere e altri dati significativi tra i quali:

- Identificativi: Seriale, MAC address, Produttore, ID.
- Sistema Operativo: Tipo, Versione, Build.
- Specifiche: Archivio, CPU, GPS, RAM, Risoluzione.
- Sicurezza: Root, criptaggio, passcode, localizzazione, modalità smarrito, antivirus
- Versione Agent
- Rete: Indirizzo IP pubblico, Indirizzo IP locale, stato Wi-Fi, SSID Wi-Fi, VPN.
- Aggiornamenti disponibili
- Gruppi: Gruppi configurati.
- Stato sicurezza: Esito scansioni anti-malware, regole firewall, blocklist siti web.
- Applicazioni: Lista delle applicazioni installate con eventuali aggiornamenti disponibili

Tra le configurazioni del dispositivo a rischio per la sicurezza è possibile visualizzare, tra le altre, anche:

- Stato del debug USB;
- Permesso di installazione applicazioni;
- Installazione app da sorgenti sconosciute;
- Modalità developer;
- Stato passcode;
- Stato criptaggio;
- Stato root;
- Informazioni sul software

Nell'immagine sottostante possiamo vedere come la console di gestione mostri le principali restrizioni applicate (o non) su un dispositivo



Tramite l'analisi di dati come restrizioni, avvisi di sicurezza, esiti delle scansioni e monitoraggio dei log Ermetix è in grado di fornire uno score sulla sicurezza di ciascun dispositivo che è consultabile nelle apposite sezioni del pannello di gestione.

Tale valore è espresso su una scala da 0 a 10 (quindi paragonabile al sistema standard di valutazione del rischio adottato anche da NIST) e consente di identificare, a colpo d'occhio, la situazione corrente relativamente alla sicurezza dei dispositivi.

Gestione dei dispositivi basata su gruppi

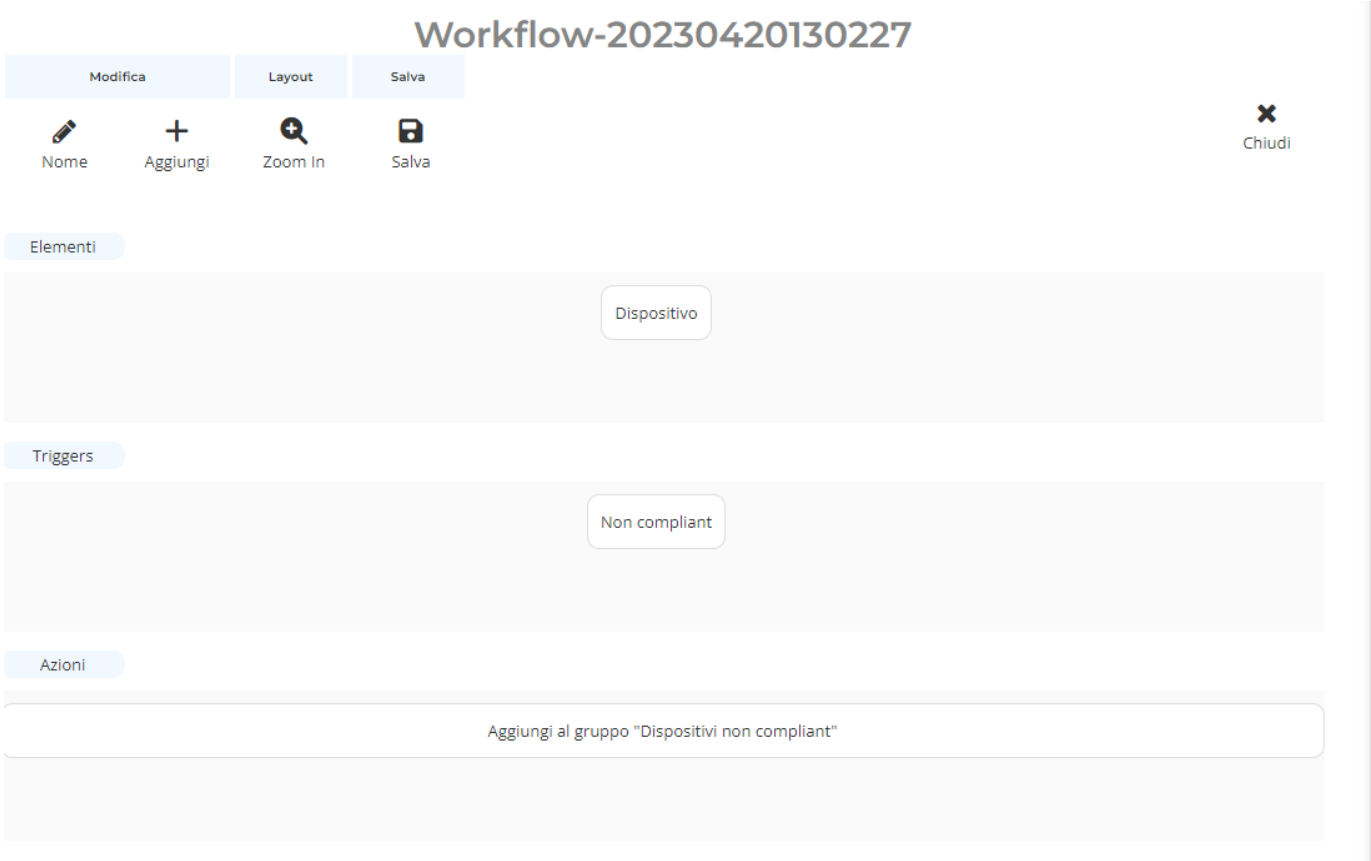
Una delle caratteristiche chiave di Ermetix è la possibilità di configurare diversi gruppi operativi, consentendo agli amministratori di organizzare e gestire i dispositivi in modo più efficiente.

All'interno del pannello di amministrazione è possibile accedere alle informazioni dettagliate di ciascun dispositivo, inclusi i gruppi operativi a cui appartengono. questo consente agli utenti di avere una visione chiara della configurazione e dell'assegnazione dei dispositivi a vari gruppi.

In particolare Ermetix permette di gestire in modo completo e modulare i dispositivi attraverso gruppi, tags, o "smart workflows".

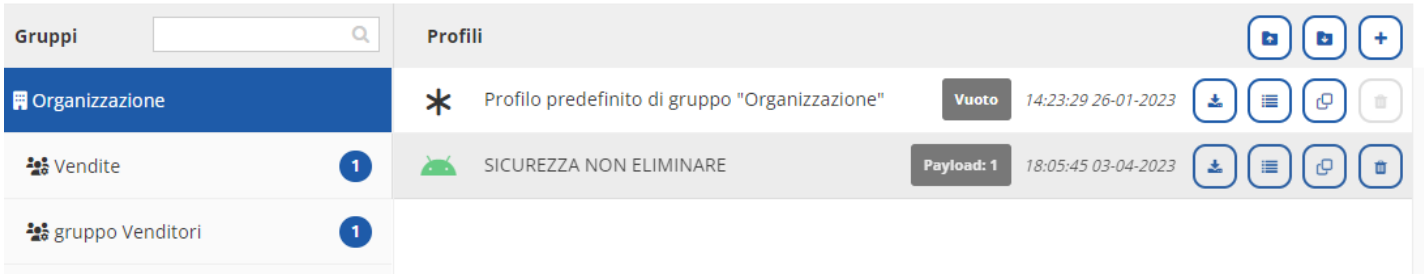
I dati disponibili sulla console di amministrazione e le politiche di hardening possono essere facilmente gestite dalla console di gestione su più dispositivi contemporaneamente attraverso gruppi personalizzati, ma non solo: è possibile creare gruppi che verranno riempiti dinamicamente in base a determinate condizioni definite da chi utilizza la console.
Esempi:

- E' possibile creare gruppi di dispositivi, manualmente, sul pannello di gestione
- Si può creare uno "smart workflow" che permette di aggiungere uno o più dispositivi a un gruppo "dinamico" al verificarsi di determinate condizioni
- Per ogni gruppo è possibile specificare policy diverse



Nell'immagine sopra viene mostrato come sia possibile aggiungere dinamicamente un dispositivo a un gruppo.

Da segnalare, anche, la possibilità di esportare ed importare tutti i profili di gruppo in formato JSON.

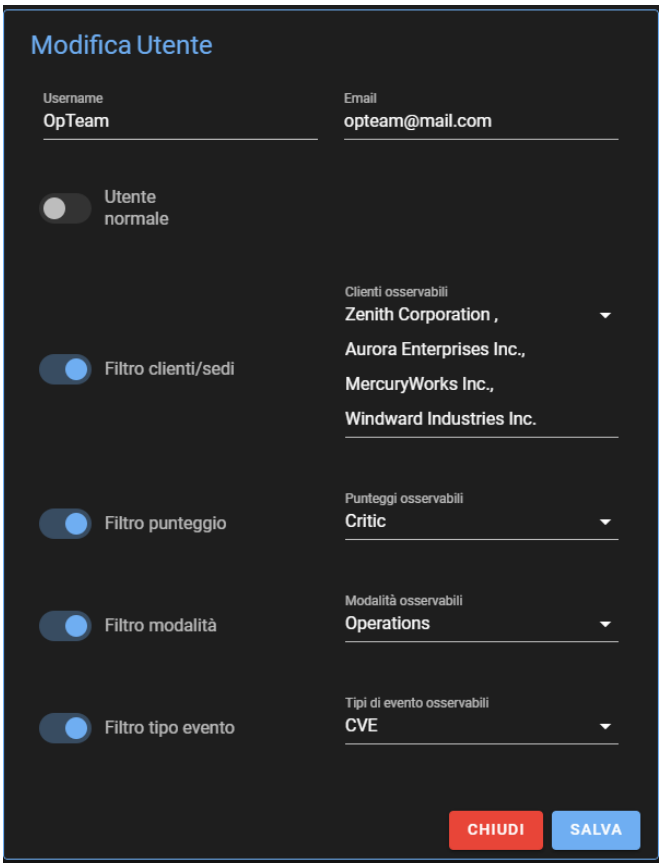


Nell'immagine sopra viene visualizzata la sezione della console di gestione che permette di creare gruppi e profili

Visualizzazione dei dati basata su permessi

La console di gestione propone alcuni ruoli preimpostati come, ad esempio, il ruolo amministratore; allo stesso tempo offre la possibilità di configurare ruoli personalizzabili assemblando gruppi di permessi. Questo è indispensabile per garantire un accesso su diversi livelli ai dati disponibili.

Basandosi sui permessi è anche possibile configurare gli avvisi e le sezioni della console da mostrare all'utente che ha eseguito il login. Forniamo un esempio nell'immagine sottostante.



Esportazione dei dati dalla console di gestione

I dati relativi alla sicurezza dei dispositivi presenti nella console di gestione sono esportabili in diversi modi; in particolare è possibile:

- esportare verso altri servizi tramite JSON o XML
- esportare i dati sotto forma di pdf o csv direttamente dal pannello
- esportare syslog raw in file .log
- sfruttare l'integrazione con servizi terzi (SIEM) con dati syslog in formato compatibile con gli standard internazionali.

Ermetix Agent sui dispositivi mobili

La procedura di installazione di Ermetix Agent su Android ed iOS, è semplificata, è possibile avviare la configurazione in maniera zero-touch, tramite l'inquadramento di un QR CODE o scaricando l'app direttamente da App Store e Play Store.

Notifiche sul dispositivo

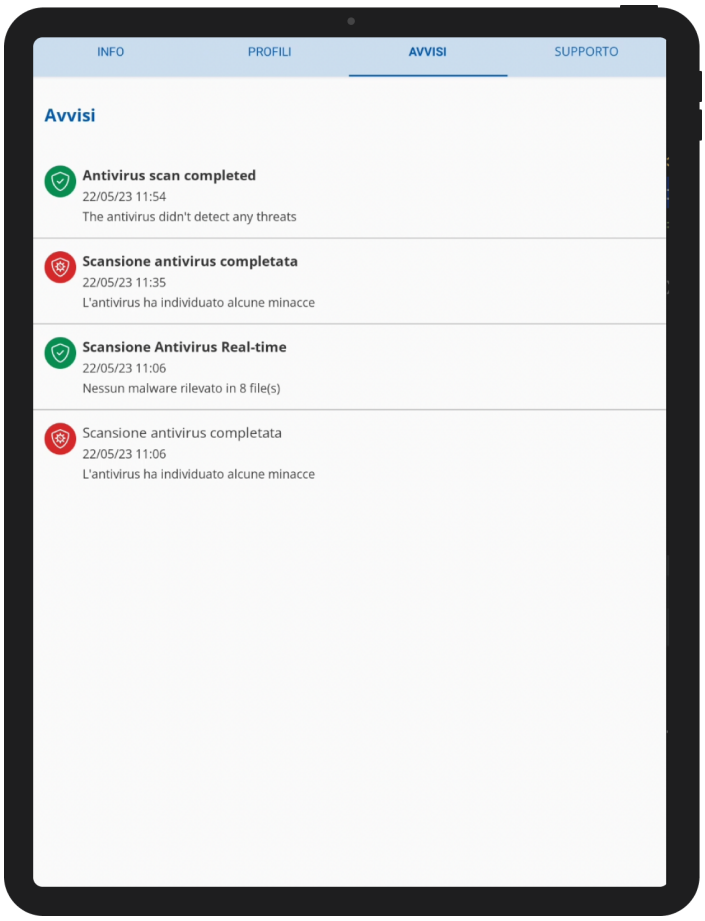
Notifiche relative alla scansione sono disponibili anche sui dispositivi mobili per mantenere l'utente finale costantemente informato. E' possibile configurare due tipi di notifiche per l'utente:

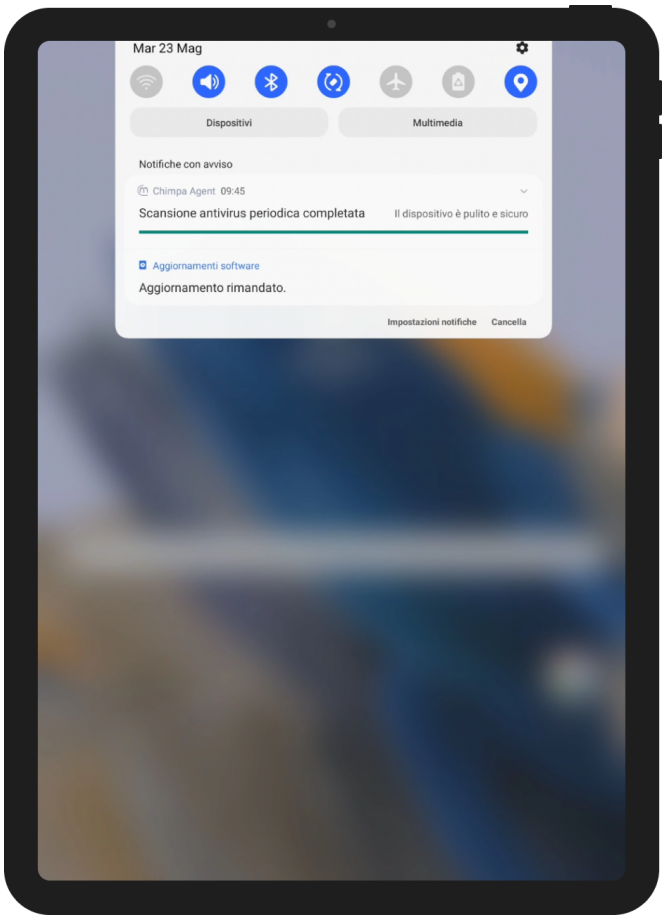
- Notifiche Popup: vengono visualizzate direttamente sullo schermo dell'utente, in modo da attirare immediatamente la sua attenzione. Queste notifiche informano l'utente su importanti aggiornamenti riguardanti le scansioni periodiche e in tempo reale dell'antivirus. Vengono segnalate l'avvio di una scansione, il completamento con successo di una scansione e la rilevazione di eventuali minacce.

- Notifiche nella sezione avvisi: vengono visualizzate all'interno della sezione dedicata agli avvisi dell'interfaccia utente dell'anti-malware. Queste notifiche forniscono un registro dettagliato degli eventi dell'antivirus, consentendo all'utente di accedere alle informazioni in qualsiasi momento. Attraverso questa sezione, l'utente può consultare lo storico delle scansioni, verificare quali minacce sono state rilevate e ottenere dettagli sugli eventuali problemi riscontrati.

Grazie all'utilizzo combinato di notifiche popup e notifiche nella sezione avvisi, il sistema garantisce una comunicazione efficace e tempestiva tra l'utente e l'amministratore, mantenendoli costantemente informati sugli eventi verificatisi e consentendo loro di prendere prontamente le misure necessarie per garantire la sicurezza del sistema.

Queste notifiche sono pre-configurate e automatiche; è, tuttavia, possibile configurare notifiche personalizzate da inviare al dispositivo direttamente dalla console di amministrazione.





Nelle immagini sopra è possibile visualizzare due diversi tipi di avvisi che vengono mostrati sui dispositivi mobili: a sinistra l'elenco delle scansioni presente nell'applicazione Ermetix, a destra una notifica visualizzabile anche a schermo bloccato.

Modalità Emergenza

La modalità di emergenza viene avviata automaticamente a seguito dell'individuazione di minacce o rischi che non possono essere rimediate automaticamente. Questo permette di contenere il malware / threat senza che possa accedere o colpire dati ed app sensibili.

L'attivazione della modalità di emergenza può essere configurata direttamente su ermetix, nei seguenti casi:

- Malwares o Threats che non possono essere automaticamente rimossi o rimediati;
- Il dispositivo è isolato dal server ermetix, da un tempo definito;
- Permessi che servono per il monitoraggio e protezione di un dispositivo, vengono manomessi o revocati
- Le regole di compliancy non sono rispettate

Condivisione dei dati sul dispositivo

Al fine di fornire una panoramica completa del comportamento dell'anti-malware e delle scansioni, Chimpa Agent invierà un messaggio in broadcast specifico al termine di ogni scansione contenente i dettagli dei file e le app analizzate via formato JSON.

Di seguito le informazioni relative all'Intent inviato in broadcast per i dispositivi Android:

Action: eu.chimpa.mdmagent.ANTIMALWARE_SCAN;
Extras: "info";

Struttura JSON dell'extra "info":

```
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;
}
```

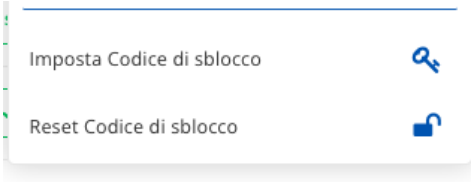
```
public class ScanJson {

    @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;
}
```

Funzionalità aggiuntive

Invio di azioni al dispositivo

Tramite il pannello web è possibile inviare alcune azioni dirette a uno o più dispositivi. Affinché l'azione venga ricevuta il dispositivo deve necessariamente essere connesso alla rete

Azioni relative alla sicurezza: Imposta/resetta Codice di sblocco, blocca schermo, Protezione Ripristino dati fabbrica, Abilita modalità smarrito



Imposta/resetta Codice di sblocco

Queste azioni consentono all'amministratore di impostare da remoto un PIN sul singolo dispositivo o di eliminarlo per poter accedere al dispositivo se non si ricorda il codice di sblocco

Blocca schermo

Questa azione blocca lo schermo se il dispositivo ha lo schermo acceso. Se il dispositivo ha un codice di sblocco configurato, questo verrà immediatamente richiesto per sbloccarlo

Abilita Protezione Ripristino Dati di Fabbrica (Android)

Con questa azione disponibile solo per Android viene richiesto di specificare un account Google. Questo account Google verrà richiesto per sbloccare il dispositivo in seguito ad un reset alle impostazioni di fabbrica. L'account Google sarà richiesto anche se il dispositivo è stato resettato tramite Hard Reset

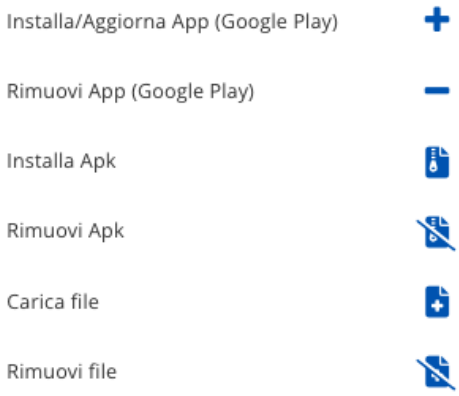
Abilita modalità smarrito (iOS)

Questa azione imposta un PIN di sblocco e abilità la modalità smarrito sull'iPhone o iPad. Sulla schermata di blocco vengono mostrate delle informazioni di contatto. Allo sblocco del telefono viene inviata la posizione esatta del dispositivo che è possibile consultare sul pannello web

Azioni relative a apps & media: installa o rimuovi app/apk, carica o elimina file

Con queste azioni è possibile selezionare una app dallo store relativo (Play Store per Android, App Store per iOS) e inviare il comando di installazione della stessa.

E' possibile inoltre, per Android, installare una **APK** fornendo un link diretto al file .apk che può risiedere su Dropbox, Google Drive o OneDrive



Nota: *affinché l'installazione della apk vada a buon fine è necessario abilitare l'opzione* ***Consenti sorgenti sconosciute*** *nelle* ***Restrizioni***

Azioni relative al dispositivo: notifica, riavvia, spegni, inizializza

Notifica

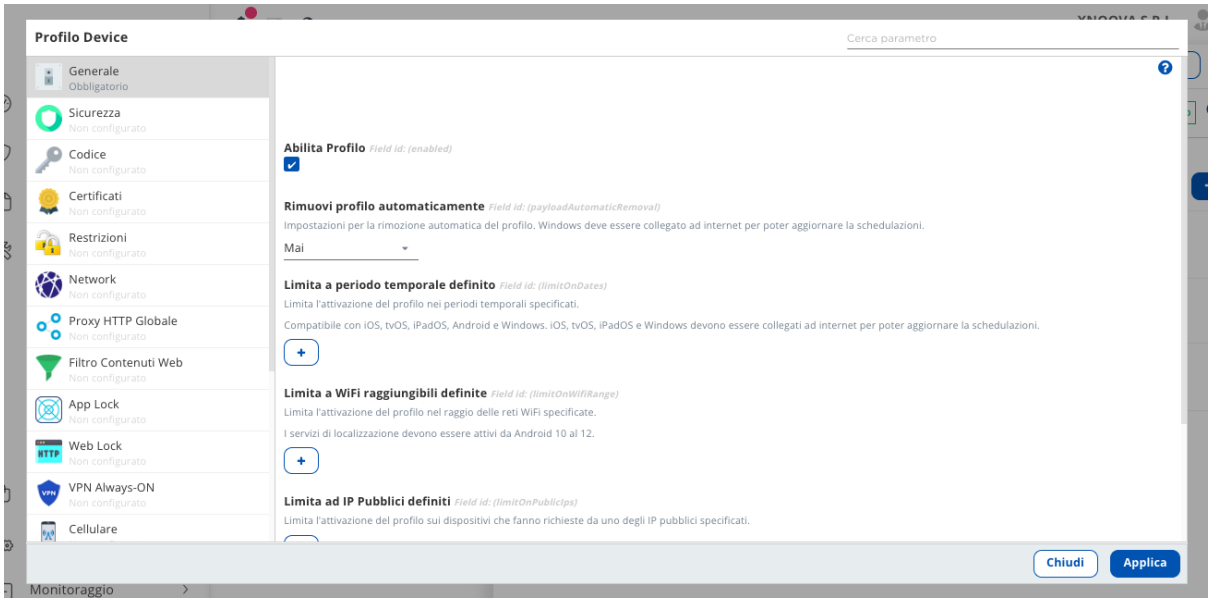
Questa azione invia un messaggio al dispositivo, che può essere una popup a schermo intero o una semplice notifica con un messaggio di testo

Inizializza

Questa azione invia un comando di reset alle impostazioni di fabbrica al dispositivo. **Attenzione:** questa azione scollega il dispositivo dal controllo remoto e deve essere nuovamente registrato

Installazione dei profili di configurazione

Con i profili di configurazione è possibile calibrare da remoto il comportamento dei dispositivi e le funzioni accessibili agli utenti che li utilizzano



Si possono ad esempio applicare **Restrizioni** come impostare una lista di app non utilizzabili, bloccare la fotocamera, inibire lo screenshoot, impedire il reset alle impostazioni di fabbrica.

Si può inoltre inviare un set di **Reti salvate** che si memorizzano sul dispositivo ed impostare che lo stesso possa connettersi solo a queste e non ad altre disponibili.

Sempre attraverso questi profili si può abilitare la **Modalità Chiosco** attraverso l'**App Lock**, che limita l'utilizzo sul dispositivo solo di alcune applicazioni, o il **Web Lock** che blocca il dispositivo su un browser aprendo un link definito. I profili possono inoltre agire su tutti gli aspetti che riguardano il dispositivo come gli **Account Google Consentiti**, il **Geofence**, la gestione dello **Sfondo** e la policy del **Codice** di sicurezza del blocca schermo

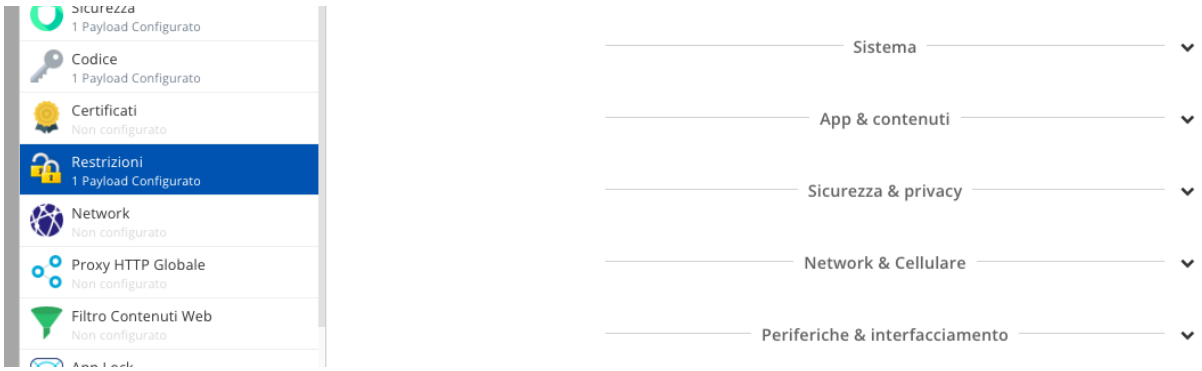
Policy Codice Blocca Schermo

Questa funzionalità imposta la policy minima di sicurezza che deve essere soddisfatta sul dispositivo. Ad esempio una policy **Bassa** permette che sul dispositivo sia sufficiente un pin di 4 caratteri numerici, una policy **Alta** invece richiede che per disattivare il blocco schermo sia necessario specificare una password con caratteri Alfanumerici

Se non viene soddisfatta la policy minima il dispositivo andrà in **Modalità emergenza** che verrà disabilitata solo inserendo il blocco schermo richiesto

Hardening dei dispositivi

Ermetix mette a disposizione **oltre 200 possibili restrizioni** che regolano l'utilizzo del dispositivo e bloccano o limitano le funzionalità a cui può accedere l'utente allo scopo di mantenere un controllo passivo sul dispositivo.

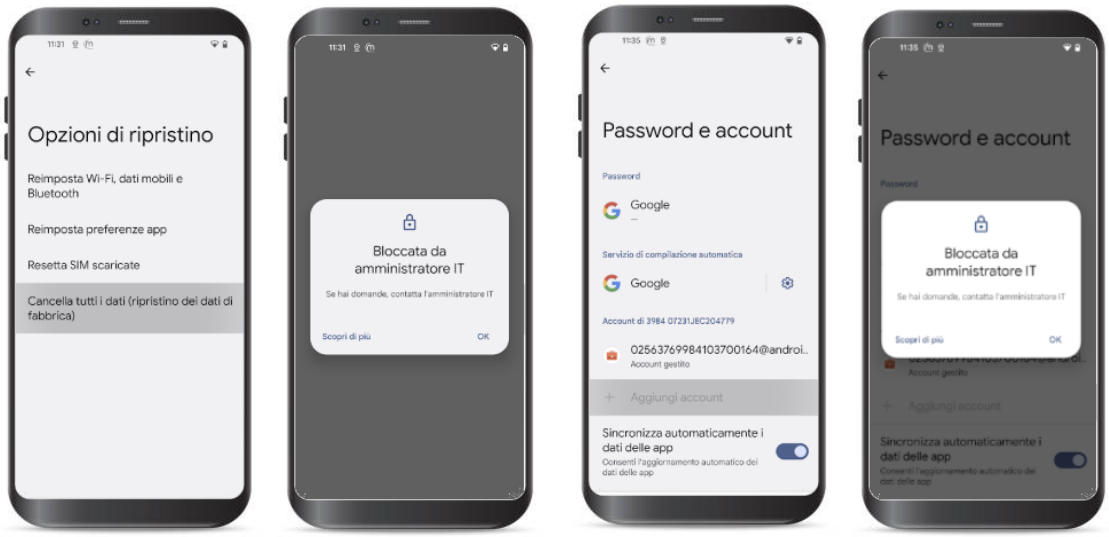


Nell'immagine sopra possiamo osservare le macro-aree in cui sono divise le restrizioni applicabili

Alcune delle restrizioni disponibili :

Sistema: inibire ripristino dati fabbrica e aggiunta account

Queste due opzioni disabilitano la possibilità per l'utente che utilizza il dispositivo di **Ripristinarlo ai dati di fabbrica** e di **Aggiungere Account**
Abilitando queste impostazioni si impedisce sia che il dispositivo esca dal controllo remoto e dalle policy impostate tramite pannello web inizializzando il dispositivo manualmente, sia che attraverso il proprio account personale si possano ad esempio installare applicazioni attraverso gli Store di app

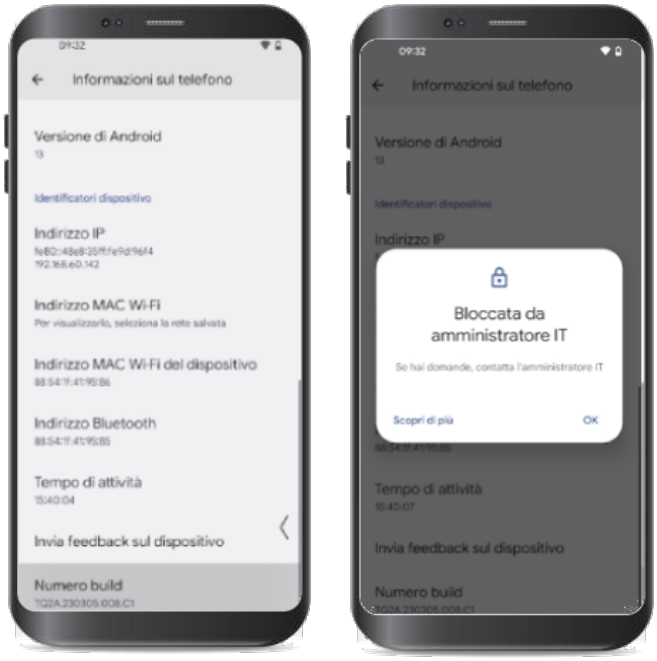


Sistema: inibire modalità sviluppatore

Tramite le restrizioni viene **bloccata** la **modalità sviluppatore** sul dispositivo.

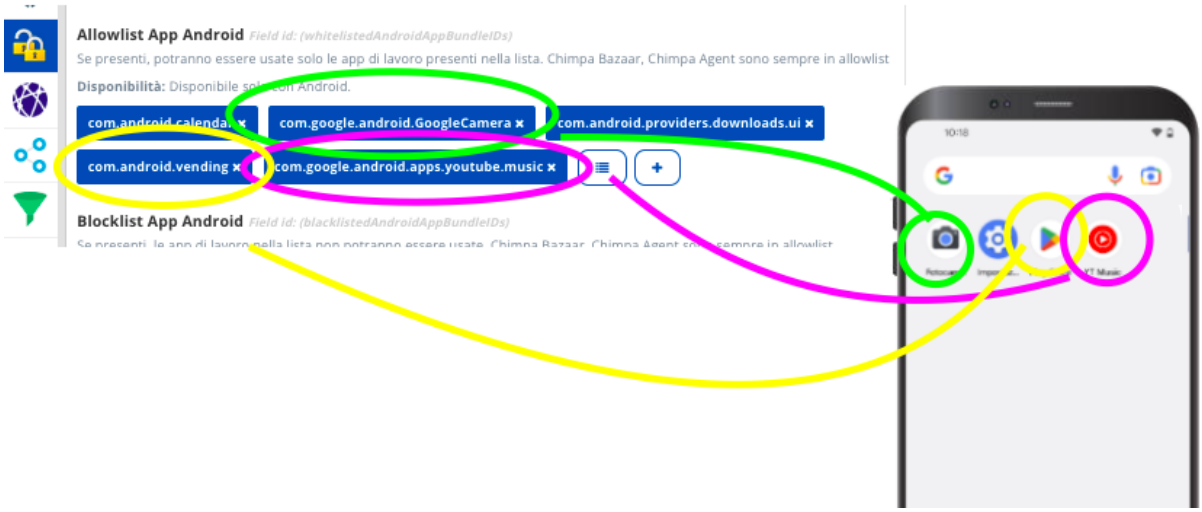
Questa modalità se attivata consente all'utente di compromettere l'integrità del dispositivo.

Attraverso le restrizioni applicate questa funzionalità viene negata di default



App & contenuti: allowlist/blocklist App

In questa sezione è possibile definire una **Allowlist**, ovvero una lista di app consentite e che quindi sono le sole a poter essere utilizzate, oppure una **Blocklist**, una lista di app che anche se installate vengono nascoste e non è possibile utilizzare



Network & cellulare: forza accesso solo a Wifi configurate

Con questa opzione si limita la connessione del dispositivo solamente alle **Wifi** configurate nello stesso profilo. Per abilitare questa opzione è necessario quindi specificare nelle **Reti salvate** almeno un **SSID** e **Password** alla quale il dispositivo può connettersi

Network & cellulare: Blocca Gestione VPN

Questa opzione **impedisce** all'utente la possibilità di modificare le impostazioni VPN o di impostare una **nuova connessione VPN**.

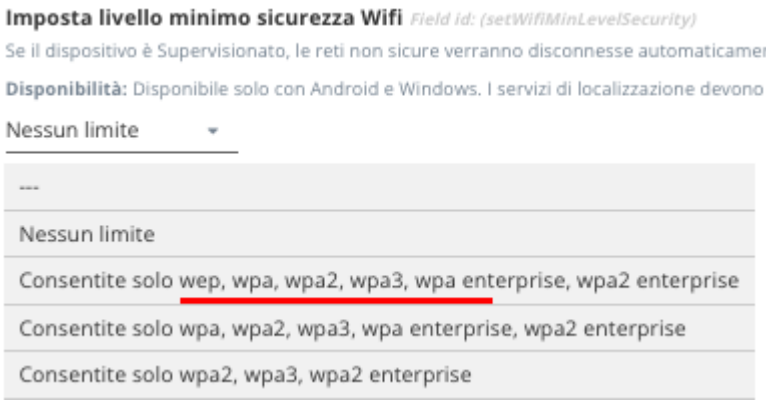
Negare questa funzionalità all'utente può essere fondamentale per garantire la sicurezza del dispositivo, che potrebbe altresì configurare una **VPN non sicura** allo scopo di accedere a contenuti generalmente non accessibili

Nota: questa funzionalità se attivata non va a disabilitare le VPN sicure già attive impostate dall'amministratore

Network & cellulare: impostare livello minimo di sicurezza consentito della password delle Reti salvate sul dispositivo

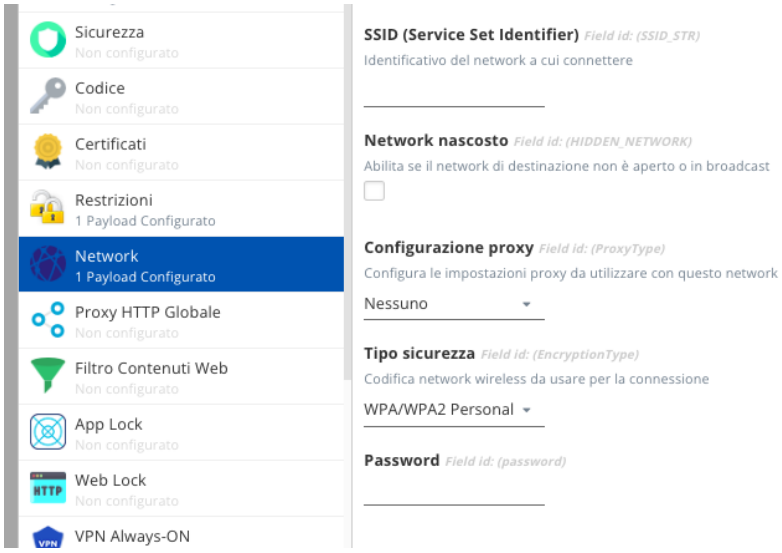
Questa opzione se impostata permette di verificare il livello di sicurezza minimo della password Wifi al quale il dispositivo si connette

E' possibile ad esempio escludere il Wifi che utilizzano criptaggio **Wep** o **Wpa** e consentire una Wifi che utilizza **Wpa2**



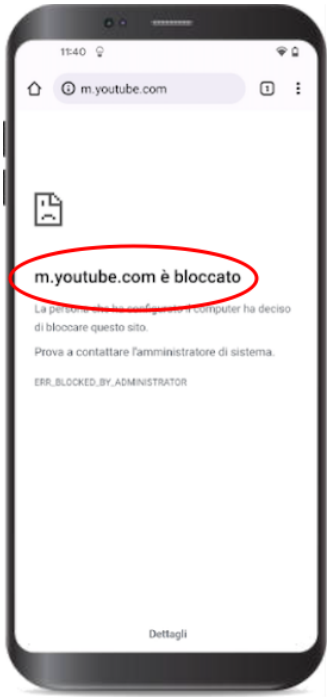
Reti salvate

Si possono definire le **Reti Salvate** specificando **SSID** e **Password**. Le reti qui definite verranno salvate sul dispositivo, alle quali potrà connettersi senza dove specificare manualmente la password



Filtro contenuti web

E' possibile definire una lista di siti web ai quali il browser di sistema del dispositivo non può accedere (**Blocklist)** o una lista limitata ai quali può accedere escludendo tutti gli altri **(Allowlist)**

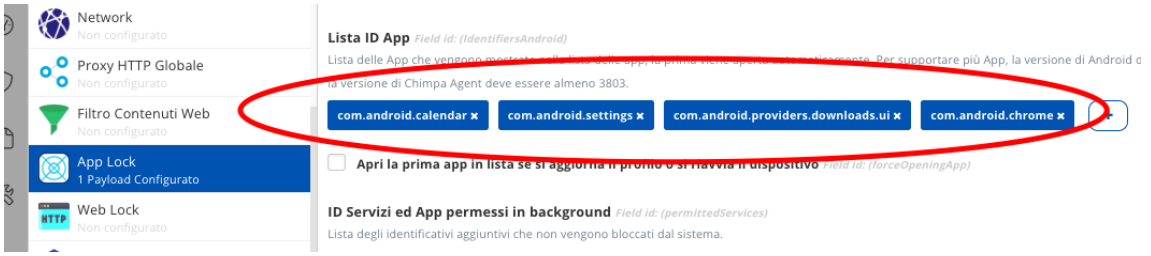


Funzionalità App lock/Web Lock

Queste funzionalità abilitano la modalità chiosco (**Kiosk mode**) sul dispositivo. Questa modalità limita l'utilizzo del dispositivo ad un elenco di applicazioni specificate.

Generalmente questa modalità viene utilizzata per dispositivi come i **Totem pubblicitari**, terminali con informazioni generiche, ma anche ad esempio tablet per effettuare ordinazioni nei ristoranti, tablet di servizio per utilizzo pubblico etc.

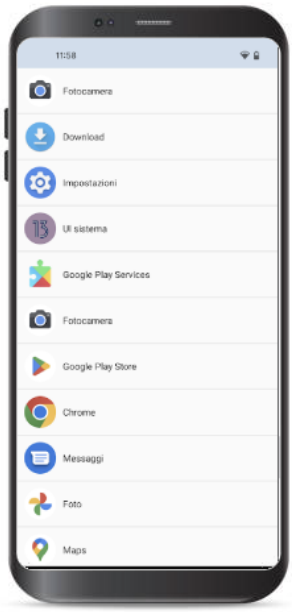
Con la funzionalità **App Lock** si definisce una lista di applicazioni da utilizzare



Una volta definito il dispositivo entrerà in **modalità chiosco** e potranno essere aperte solamente le app specificate

Il dispositivo rimarrà in questo stato fin quando non viene rimosso il profilo

La funzionalità **Web Lock** funziona alla stessa maniera, con la differenza che va specificato un **URL**

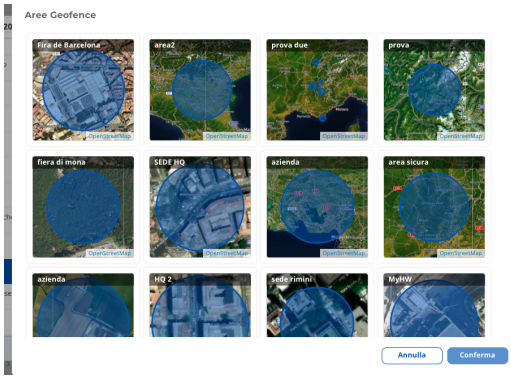


Modalità App Lock

Modalità Web Lock

Geofencing

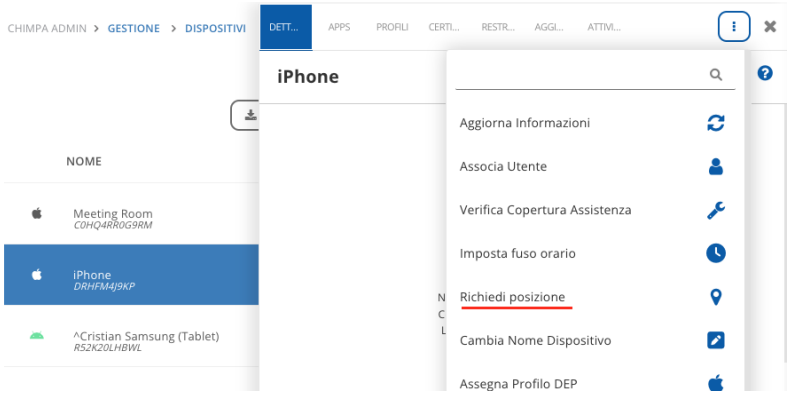
Questa funzionalità comunica al dispositivo le aree geografiche di controllo da attivare sul dispositivo. Abilitando queste aree si possono utilizzare diverse funzionalità, ad esempio la ricezione di una email di notifica quando il dispositivo entra o esce dall'area oppure l'abilitazione di alcune configurazioni solo quando il dispositivo si trova in queste aree

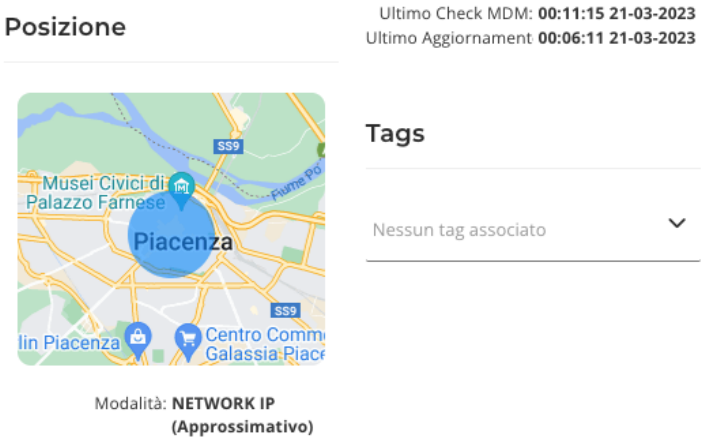


Richiedi posizione

E' possibile richiedere la **posizione** dal pannello web. La posizione verrà quindi mostrata sul pannello nella scheda dei dettagli del dispositivo

Questa funzionalità può risultare utile per identificare la **posizione** con un discreto margine di precisione del dispositivo, calcolata triangolando la posizione ottenuta tramite **Network IP** e **GPS**





Blocco periferiche esterne

Ermetix , rende possibile il controllo totale dell'accesso sia fisico sia attraverso connessioni al dispositivo , di dati provenienti da memorie di massa esterne (USB mass storage, SD Card ecc.) oppure da connessioni di prossimità come Bluetooth ed NFC .
Infatti è possibile configurare

Questa funzionalità può risultare molto utile per evitare sia che questo tipo di accessi diventino vettori di possibili "infezioni" di malware, sia per evitare esfiltrazioni di dati critici dai device presi di mira.