ESET ENDPOINT SECURITY for ANDROID

Manuale dell'utente

(per la versione 2.0 e le versioni successive del prodotto)

Fare clic qui per scaricare la versione più recente di questo documento

ESET **ENDPOINT SECURITY**

Supporto tecnico: http://www.eset.it/supporto/assistenza-tecnica

REV. 28. 8. 2015

Contenuti

1. Introduzione

La nuova generazione di ESET Endpoint Security for Android (EESA) è stata pensata per funzionare insieme a ESET Remote Administrator (ERA) 6, la nuova console di gestione che offre una gestione remota di tutte le soluzioni di protezione ESET. ESET Endpoint Security for Android 2 è compatibile solo con ERA 6 e versioni successive.

ESET Endpoint Security for Android è stato pensato per proteggere i dispositivi mobili aziendali e i dati dalle minacce malware più recenti in caso di furto o smarrimento. Il programma è pensato anche per aiutare gli amministratori di sistema a garantire la conformità dei dispositivi alle politiche di sicurezza aziendali.

ESET Endpoint Security può essere utilizzato anche da aziende di piccole-medie dimensioni senza la necessità di una gestione remota attraverso ESET Remote Administrator. Tecnici informatici, amministratori di sistema o gli utenti effettivi dell'Endpoint possono condividere la configurazione di ESET Endpoint Security in modo semplice con altri colleghi. Questo processo elimina completamente il bisogno di attivare il prodotto e di configurare manualmente ciascun modulo del prodotto richiesto in seguito all'installazione di ESET Endpoint Security.

1.1 Novità della versione 2

Controllo applicazione

Il Controllo applicazione consente agli amministratori di monitorare le applicazioni installate, bloccare l'accesso ad applicazioni definite e ridurre il rischio di esposizione suggerendo agli utenti la disinstallazione di specifiche applicazioni. Per ulteriori informazioni, consultare la sezione Controllo applicazione della presente guida.

Protezione dispositivo

La protezione dispositivo consente agli amministratori di eseguire criteri di protezione di base su dispositivi mobili multipli. Ad esempio, a un amministratore è consentito di:

- impostare il livello di protezione minimo e la complessità dei codici di blocco della schermata
- impostare il numero massimo di tentativi di sblocco non riusciti
- impostare l'intervallo di tempo in seguito al quale gli utenti devono modificare il proprio codice di blocco della schermata
- impostare il timer per il blocco della schermata
- limitare l'utilizzo della fotocamera

Per ulteriori informazioni, consultare la sezione Protezione dispositivo della presente guida.

Importazione ed esportazione delle impostazioni

Per un'agevole condivisione delle impostazioni tra due dispositivi mobili non gestiti da ERA, ESET Endpoint Security 2 introduce la possibilità di esportare e di importare le impostazioni del programma. L'amministratore può esportare manualmente le impostazioni del dispositivo in un file che è possibile condividere (ad esempio, tramite e-mail) e importare in qualsiasi dispositivo su cui è in esecuzione l'applicazione client. Nel momento in cui l'utente accetta il file delle impostazioni ricevuto, definisce automaticamente tutte le impostazioni e attiva l'applicazione (a condizione che siano state incluse le informazioni sulla licenza). Tutte le impostazioni sono protette dalla password amministratore.

Anti-Phishing

Questa funzione protegge gli utenti da accessi a siti Web dannosi in caso di utilizzo di browser Web supportati (browser Android predefinito e Chrome).

La tecnologia Anti-Phishing protegge gli utenti da tentativi di acquisizione di password, informazioni bancarie e altri dati sensibili da parte di siti Web illegali camuffati da siti legittimi. Se un dispositivo tenta di accedere a un URL, ESET Anti-Phishing lo confronta con il database ESET di siti phishing noti. In caso di corrispondenza, la connessione all'URL viene interrotta e compare un messaggio di avviso.

Centro notifiche

ESET Endpoint Security offre agli utenti un centro notifiche unificato in cui sono disponibili tutte le notifiche relative alle funzioni dell'applicazione che richiedono attenzione. Il centro notifiche fornirà informazioni sui vari eventi, i motivi alla base della mancata conformità alle politiche aziendali e le misure da attuare per impedire la violazione di tali requisiti. Le notifiche vengono organizzate in base alla priorità (ordinamento decrescente).

Nuovo sistema di gestione delle licenze

ESET Endpoint Security supporta tutte le funzionalità di ESET License Administrator, che rappresenta il nuovo modello di gestione delle licenze introdotto con ESET Remote Administrator 6.

Una nuova infrastruttura di gestione delle licenze semplifica l'utilizzo a lungo termine del software di protezione ESET. Le eventuali modifiche alla licenza richieste dai clienti saranno applicate in modo automatico e trasparente su tutti i prodotti legati a quella specifica licenza. Questa opzione consente agli utenti di utilizzare i propri indirizzi e-mail e una password personalizzata come credenziali, anziché il nome utente e la password ESET utilizzati per le versioni precedenti dei prodotti.

L'introduzione delle chiavi di licenza e degli aggiornamenti automatici delle licenze (a fronte del rinnovo e di altre operazioni relative alla licenza) garantisce agli utenti un livello di protezione adeguato. Il portale ESET License Administrator e la capacità di assegnare i diritti relativi all'autorizzazione della licenza attraverso l'indirizzo di posta elettronica (sulla base delle informazioni sugli account degli utenti) semplificano la gestione e l'utilizzo delle licenze. ESET License Administrator consente ai proprietari di licenza di delegarne la gestione a un'entità responsabile, persino una terza parte, senza perderne il controllo.

Gestione dell'aggiornamento della build di un prodotto

Gli amministratori di sistema che utilizzano ERA e non desiderano installare l'ultima versione di ESET Endpoint Security per Android non appena disponibile hanno la possibilità di controllare il meccanismo di aggiornamento.

Procedure guidate di configurazione

ESET Endpoint Security offre procedure guidate di post-installazione per funzioni selezionate allo scopo di semplificare il processo.

Protezione antivirus potenziata

- Tempi di controllo in tempo reale potenziati (all'accesso)
- ESET Live Grid integrato
- 2 livelli di controllo: intelligente e approfondito
- Controllo su richiesta in background potenziato e possibilità di sospensione del controllo
- Possibilità di pianificazione del controllo completo di un dispositivo da parte dell'amministratore
- Controllo durante il caricamento: si avvierà automaticamente un controllo se il dispositivo si trova nello stato inattivo (completamente carico e collegato a un caricatore).
- Configurazione avanzata degli aggiornamenti del database delle firme antivirali: l'amministratore può specificare gli intervalli di tempo degli aggiornamenti periodici e selezionare il server di aggiornamento utilizzato dai dispositivi (server di rilascio, server di pre-rilascio, mirror locale)

I rapporti dettagliati contenenti i risultati dei controlli vengono inviati a ERA. ESET Endpoint Security include funzioni previste dalla versione 1 di ESET Endpoint Security, come il rilevamento di applicazioni potenzialmente pericolose, il rilevamento delle applicazioni potenzialmente indesiderate e l'USSD Control.

Filtro SMS e chiamate potenziato

Il filtro SMS e chiamate, noto in precedenza con il nome di antispam, protegge gli utenti da chiamate e messaggi SMS ed MMS indesiderati. Questa funzione offre attualmente due tipi di regole: regole dell'amministratore e regole dell'utente, dove le prime sono sempre superiori rispetto alle seconde.

Altri miglioramenti includono:

- Blocco temporale: l'utente o l'amministratore ha la possibilità di bloccare le chiamate e i messaggi ricevuti a orari specificati
- Blocco con un solo tocco per l'ultimo ID chiamante o mittente dei messaggi, numero di telefono, gruppo di contatti e numeri nascosti o sconosciuti

Funzione Anti-Furto potenziata

Le funzioni Anti-Furto consentono agli amministratori di proteggere e individuare un dispositivo smarrito o rubato. Le misure Anti-Furto possono essere attivate da ERA o tramite comandi remoti.

ESET Endpoint Security 2 utilizza gli stessi comandi remoti della versione 1 (Blocca, Cancella e Trova). Sono stati aggiunti i seguenti comandi:

- **Sblocca**: sblocca il dispositivo bloccato
- **Ripristino avanzato impostazioni predefinite**: tutti i dati accessibili sul dispositivo verranno rimossi velocemente (le intestazioni dei file verranno distrutte) e sul dispositivo verranno ripristinate le impostazioni predefinite
- **Sirena**: il dispositivo smarrito verrà bloccato e verrà emesso un suono molto acuto anche in modalità silenziosa

Per potenziare il livello di sicurezza dei comandi remoti, l'amministratore riceverà un codice SMS di verifica univoco e con un periodo di validità limitato sul proprio telefono cellulare (al numero definito nell'elenco di contatti dell'amministratore) durante l'esecuzione di un comando remoto. Questo codice di verifica verrà utilizzato per la verifica di un comando specifico.

Comandi Anti-Furto da ERA

I comandi Anti-Furto possono ora essere eseguiti anche da ERA. La nuova funzionalità per la gestione dei dispositivi mobili consente agli amministratori di inviare comandi Anti-Furto in pochi semplici clic. Le attività vengono inviate immediatamente per l'esecuzione attraverso il connettore di dispositivi mobili che è ora parte dell'infrastruttura ERA.

Contatti dell'amministratore

Elenco dei numeri di telefono dell'amministratore protetti dalla password amministratore. I comandi Anti-Furto possono essere inviati solo da numeri attendibili.

Visualizza messaggio da ERA

In caso di gestione dei dispositivi da remoto, l'amministratore può inviare un messaggio personalizzato a un dispositivo o a un gruppo di dispositivi specifico. Tale funzione consente di comunicare un messaggio urgente agli utenti dei dispositivi gestiti. Il messaggio verrà visualizzato sotto forma di popup, per evitare che venga perso.

Blocco delle informazioni personalizzate sulla schermata

L'amministratore è in grado di definire informazioni personalizzate (ragione sociale, indirizzo di posta elettronica, messaggio) che verranno visualizzate quando il dispositivo è bloccato, con la possibilità di chiamare uno dei contatti amministratore predefiniti.

Gestione remota potenziata con ESET Remote Administrator **6**

Da oggi, è possibile configurare e definire tutte le impostazioni dell'applicazione attraverso criteri remoti, tra cui antivirus, filtro SMS e chiamate, impostazioni di protezione del dispositivo, restrizioni relative al controllo dell'applicazione e così via. Questa funzione consente agli amministratori di attuare le politiche di sicurezza aziendali sull'intera rete, compresi i dispositivi mobili.

ESET Endpoint Security for Android versione 2 offre un sistema di segnalazione potenziato visibile da ERA Web Console. Ciò consente agi amministratori di identificare prontamente dispositivi problematici e di individuare l'origine del problema.

La gestione dei dispositivi Android è ora parte integrante di ESET Remote Administrator 6 e presenta all'incirca le stesse funzioni disponibili per i prodotti desktop ESET come ESET Endpoint Antivirus 6 e ESET Endpoint Security 6.

Amministrazione locale

ESET Endpoint Security for Android offre agli amministratori la possibilità di configurare e gestire localmente gli endpoint nel caso in cui scelgano di non utilizzare ESET Remote Administrator. Tutte le impostazioni dell'applicazione sono protette dalla password amministratore per consentirne un controllo completo ininterrotto.

Distribuzione e installazione potenziate del prodotto

In aggiunta ai metodi di installazione tradizionali (download e installazione di un pacchetto dal sito Web ESET, distribuzione del pacchetto di installazione tramite e-mail), gli amministratori e gli utenti hanno la possibilità di scaricare e installare l'applicazione da Google Play Store.

Attivazione potenziata del prodotto

In seguito al download e all'installazione, l'amministratore o l'utente ha a disposizione svariate opzioni di attivazione del prodotto:

- utilizzo delle nuove opzioni di gestione delle licenze e inserimento manuale della chiave di licenza o dell'account Security Admin.
- Possibilità di fare clic sul collegamento inviato in un messaggio di posta elettronica dall'amministratore. Il prodotto configurerà automaticamente la connessione a ERA che eseguirà un push sul dispositivo delle informazioni di licenza.
- L'amministratore può inserire manualmente le informazioni relative alla connessione ERA.
- L'importazione del file contenente le impostazioni dell'applicazione (che includono le informazioni sulla licenza) determinerà quindi l'attivazione dell'applicazione.

Identificazione potenziata del dispositivo mobile in ERA

Durante il processo di registrazione, i dispositivi Android vengono inseriti in una whitelist. Di conseguenza, solo i dispositivi autorizzati potranno effettuare la connessione a ERA. Questa funzione potenzia la protezione e semplifica l'identificazione dei singoli dispositivi (ciascun dispositivo mobile viene identificato attraverso il nome, la descrizione e il codice IMEI). I dispositivi su cui è attiva esclusivamente una connessione Wi-Fi vengono identificati attraverso il rispettivo indirizzo Wi-Fi MAC.

Interfaccia utente grafica rinnovata

ESET Endpoint Security offre un'esperienza utente potenziata simile a quella disponibile in tutte le soluzioni ESET per i clienti business.

Facilità di utilizzo

La nuova interfaccia utente grafica facilita l'utilizzo e la navigazione del prodotto. La struttura della GUI è compatibile con la nuova generazione di soluzioni ESET Endpoint ed ESET Remote Administrator.

1.2 Requisiti minimi di sistema

Per installare ESET Endpoint Security su un dispositivo Android, sono necessari i seguenti requisiti minimi di sistema:

- Sistema operativo: Android 4 (Ice Cream Sandwich) e versioni successive
- Risoluzione touchscreen: 480 x 800 px
- CPU: ARM con set di istruzioni ARMv7, x86 Intel Atom
- Spazio di archiviazione: 20 MB
- Connessione Internet

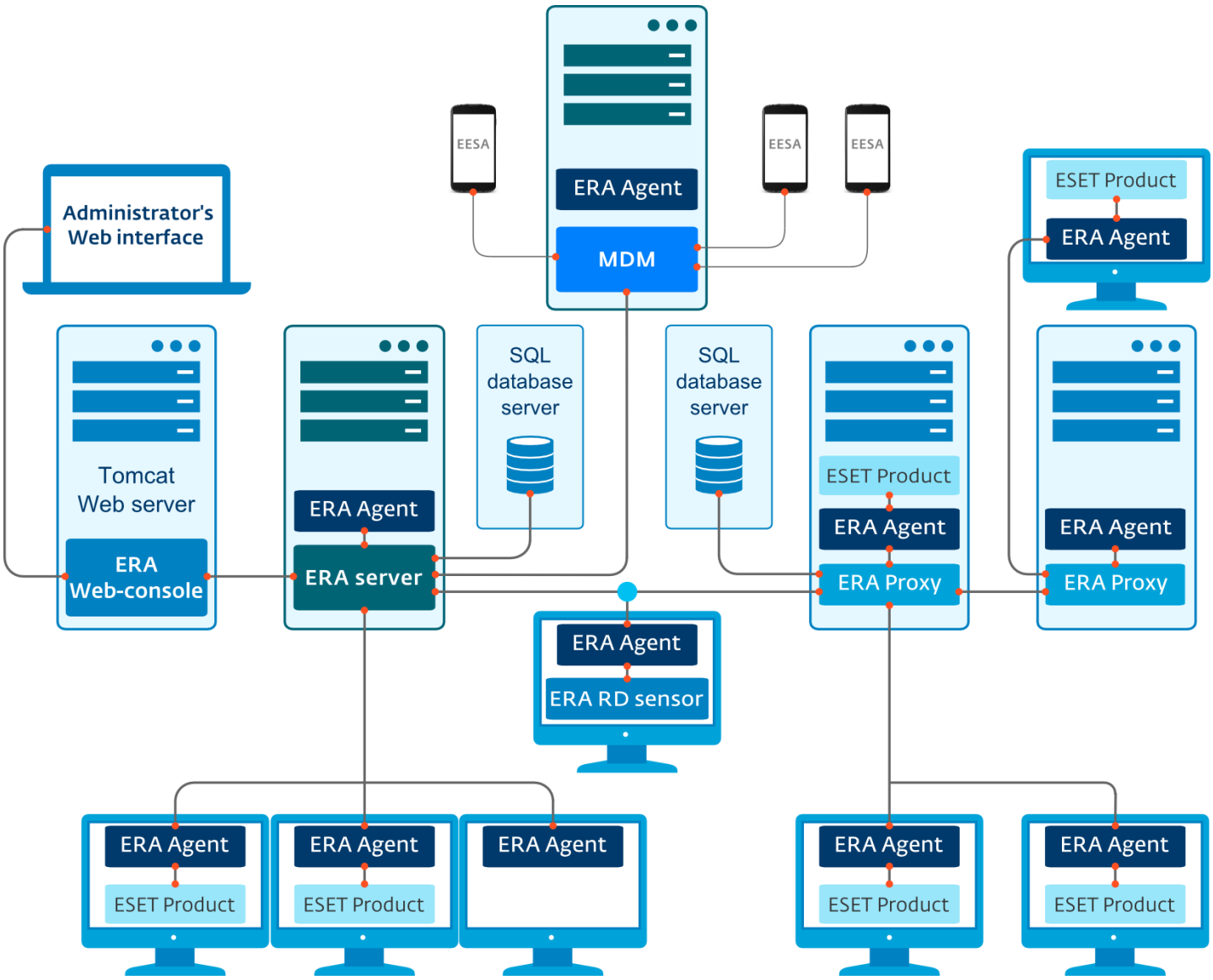
NOTA: i dispositivi dual SIM e con radice non sono supportati. Alcune funzioni (ad esempio, Anti-Furto e filtro SMS e chiamate) non sono disponibili sui tablet che non supportano i servizi di chiamata e di messaggistica.

2. Utenti che si connettono a ESET Remote Administrator

ESET Remote Administrator (ERA) 6 è un'applicazione che consente all'utente di gestire i prodotti ESET in un ambiente di rete da una postazione centrale. Il sistema di gestione delle attività ESET Remote Administrator consente all'utente di installare soluzioni di protezione ESET su computer remoti e dispositivi mobili e di rispondere rapidamente ai nuovi problemi e alle nuove minacce. ESET Remote Administrator non offre di per sé protezione contro codici dannosi, ma si affida alla presenza di una soluzione di protezione ESET su ciascun client.

Le soluzioni di protezione ESET supportano reti che includono vari tipi di piattaforme. Una rete può integrare, ad esempio, una combinazione degli attuali sistemi operativi Microsoft, Linux e OS X e dei sistemi operativi eseguiti sui dispositivi mobili (cellulari e tablet).

L'immagine sottostante illustra un esempio di architettura per una rete protetta mediante soluzioni di protezione ESET gestite da ERA:



NOTA: per ulteriori informazioni, consultare la documentazione on-line di ESET Remote Administrator.

2.1 Server ESET Remote Administrator

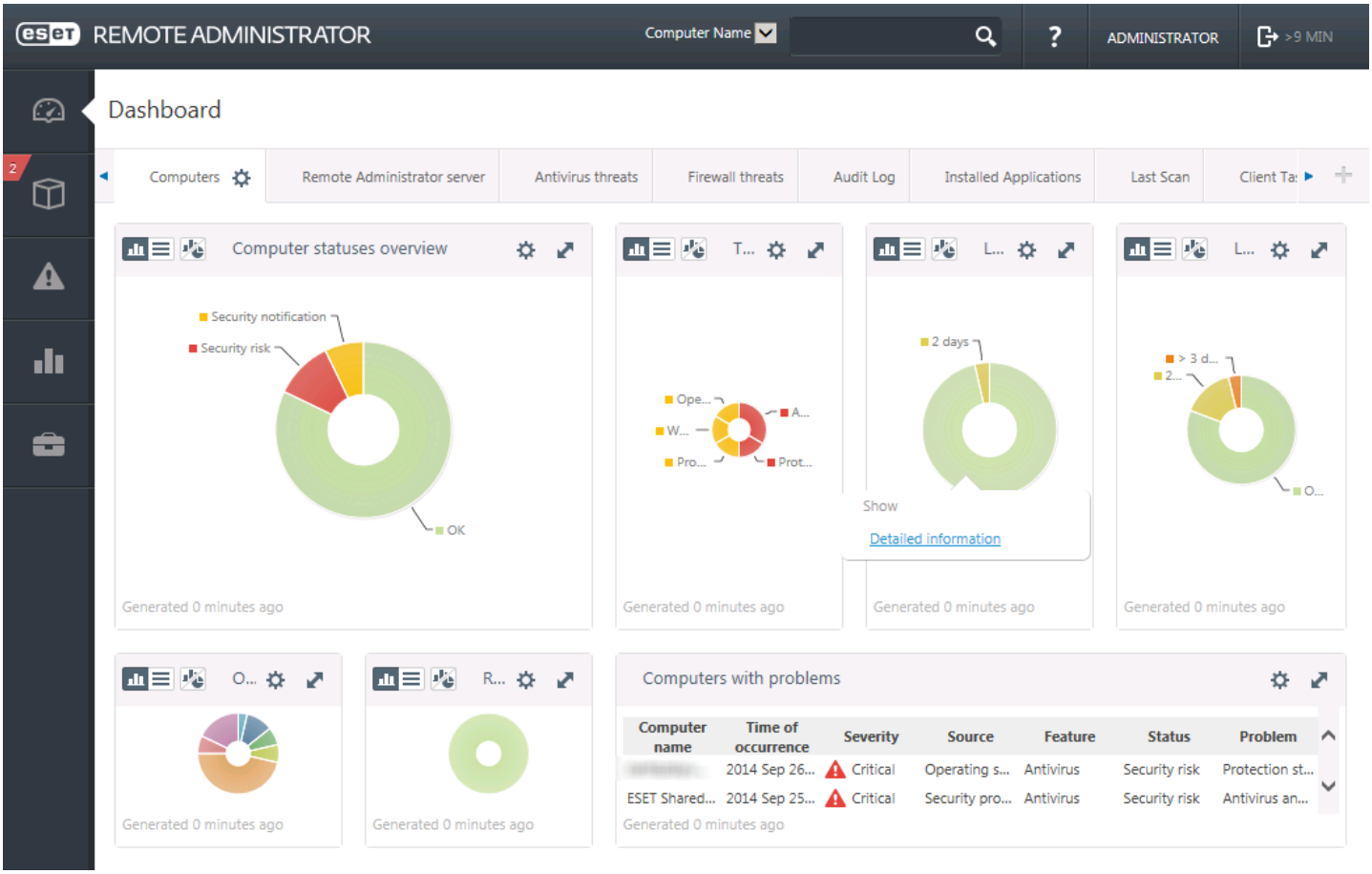
ESET Remote Administrator Server è il componente esecutivo di ESET Remote Administrator. Elabora tutti i dati ricevuti dai client che si connettono al server (attraverso l'Agente ERA). L'agente ERA facilita le comunicazioni tra il client e il server. I dati (rapporti del client, configurazione, replica dell'agente, ecc.) sono archiviati in un database a cui ERA ha accesso per fornire le segnalazioni.

Per una corretta elaborazione dei dati, il server ERA richiede una connessione stabile al server di un database. Per ottenere prestazioni ottimali, si consiglia di installare il server ERA e il database su server separati. È necessario configurare la macchina sulla quale è installato il server ERA in modo da accettare tutte le connessioni dell'agente, del proxy o di RD Sensor, che vengono verificate mediante l'utilizzo dei certificati. Dopo aver installato il server ERA, è possibile aprire ERA Web Console che consente all'utente di gestire le workstation dell'endpoint con le soluzioni ESET installate.

2.2 Console Web

ERA Web Console è un'interfaccia utente basata sul Web che presenta i dati provenienti dal Server ERA e consente all'utente di gestire le soluzioni di protezione ESET nella rete in uso. È possibile accedere alla console Web tramite un browser. che consente di visualizzare una panoramica dello stato dei client sulla rete e di utilizzare da remoto soluzioni ESET su computer non gestiti. È possibile decidere di rendere il server Web accessibile da Internet per consentire l'utilizzo di ESET Remote Administrator praticamente da qualsiasi posizione o dispositivo.

Dashboard della console Web:



Nella parte superiore della console Web, è disponibile lo strumento **Ricerca rapida**. Nel menu a discesa, selezionare **Nome computer**, **Indirizzo IPv4/IPv6** oppure **Nome minaccia**, digitare la stringa di ricerca nel campo di testo e fare clic sul simbolo della lente di ingrandimento oppure premere **Invio** per avviare la ricerca. L'utente verrà reindirizzato alla sezione **Gruppi**, dove sarà possibile visualizzare i risultati della ricerca.

2.3 Proxy

Il **Proxy ERA** è un altro componente di ESET Remote Administrator che consente di soddisfare due importanti requisiti. In reti di medie dimensioni o aziendali caratterizzate dalla presenza di numerosi client (ad esempio, 10.000 client o più), è possibile utilizzare il proxy ERA per distribuire il carico tra molteplici proxy ERA, allo scopo di facilitare i compiti del Server ERA principale. L'altro vantaggio del proxy ERA consiste nella possibilità di utilizzarlo per connettersi a una filiale aziendale da remoto con un collegamento debole. Ciò significa che l'agente ERA su ciascun client non si connette al server ERA principale direttamente attraverso il proxy ERA che si trova sulla stessa rete locale della filiale. Questa configurazione libera il collegamento alla filiale. Il proxy ERA accetta connessioni da tutti gli agenti ERA locali, ne compila i dati e li carica sul server ERA principale (o un altro proxy ERA). Tale operazione consente alla rete di adattare altri client senza compromettere le proprie prestazioni e la qualità delle query relative al database.

In base alla configurazione della rete in uso, il proxy ERA può connettersi a un altro proxy ERA per poi connettersi al server ERA principale.

Per un corretto funzionamento del proxy ERA, il computer host sul quale è stato installato il proxy ERA deve prevedere un agente ESET installato ed essere connesso al livello superiore (l'eventuale server ERA o un proxy ERA superiore) della rete in uso.

2.4 Agente

L'**Agente ERA** costituisce una parte essenziale del prodotto ESET Remote Administrator. Le soluzioni di protezione ESET sulle macchine client (ad esempio, ESET Endpoint Security) comunicano con il server ERA attraverso l'agente. Queste comunicazioni rendono possibile la gestione delle soluzioni di protezione ESET su tutti i client remoti da una posizione centrale. L'agente raccoglie informazioni dal client e le invia al server. Se il server invia un'attività a un client, ciò significa che l'attività viene inviata all'agente che comunica quindi con il client. Tutte le comunicazioni di rete avvengono tra l'agente e la parte superiore della rete ERA, ovvero il server e il proxy.

Per connettersi al server, l'agente ESET utilizza uno dei tre metodi seguenti:

1. L'agente del client è connesso direttamente al server.
2. L'agente del client è connesso mediante un proxy a sua volta connesso al server.
3. L'agente del client si connette al server mediante proxy multipli.

L'agente ERA comunica con le soluzioni ESET installate su un client, raccoglie informazioni dai programmi installati su quel client e passa le informazioni di configurazione ricevute dal server al client.

NOTA: il proxy ESET possiede il proprio agente che gestisce tutte le attività di comunicazione tra i client, altri proxy e il server ERA.

2.5 RD Sensor

RD (Rogue Detection) Sensor è un componente di ESET Remote Administrator pensato per ricercare computer all'interno della rete in uso. RD Sensor consente all'utente di aggiungere facilmente nuovi computer in ESET Remote Administrator senza la necessità di trovarli e aggiungerli manualmente. Ogni computer trovato nella rete viene visualizzato nella console Web e aggiunto al gruppo predefinito Tutti. Da qui, è possibile eseguire ulteriori azioni con singoli computer client.

RD Sensor è un ascoltatore passivo che rileva i computer presenti nella rete e invia le relative informazioni al server ERA. Il server ERA valuta se i PC trovati nella rete sono sconosciuti o già gestiti.

3. Installazione remota

L'installazione remota di ESET Endpoint Security da ERA richiede i seguenti requisiti:

- Installazione del connettore dispositivi mobili
- Registrazione dispositivi mobili

L'installazione di ESET Endpoint Security può essere eseguita in due diversi modi:

1. L'amministratore invia il collegamento della registrazione agli utenti finali tramite e-mail insieme al file di installazione APK e una breve spiegazione delle modalità di installazione. Toccando il collegamento, gli utenti vengono reindirizzati al browser Internet predefinito del proprio dispositivo Android e ESET Endpoint Security saranno registrati e connessi a ERA. Se ESET Endpoint Security non è installato sul dispositivo, gli utenti verranno reindirizzati automaticamente a Google Play Store per il download dell'app. A questa operazione seguirà un'installazione standard.
2. L'amministratore invia il file delle impostazioni dell'applicazione agli utenti finali tramite e-mail insieme al file di installazione APK e una breve spiegazione delle modalità di installazione. In alternativa, agli utenti verrà richiesto di scaricare il file APK da Google Play Store, il cui collegamento verrà fornito dall'amministratore. In seguito all'installazione, gli utenti aprono il file delle impostazioni dell'applicazione. Tutte le impostazioni verranno importate e l'applicazione verrà attivata (a condizione che siano state incluse le informazioni sulla licenza).

4. Installazione locale sul dispositivo

ESET Endpoint Security offre agli amministratori la possibilità di configurare e gestire localmente l'endpoint nel caso in cui scelgano di non utilizzare ESET Remote Administrator. Tutte le impostazioni dell'applicazione sono protette dalla password amministratore per consentire un controllo completo e ininterrotto in termini di amministrazione.

Se un amministratore all'interno di un'azienda di piccole dimensioni decide di non utilizzare ESET Remote Administrator ma desidera ancora proteggere i dispositivi aziendali e applicare criteri di sicurezza di base, ha a disposizione due opzioni per la gestione locale dei dispositivi:

1. Accesso fisico a ciascun dispositivo aziendale e configurazione manuale delle impostazioni.
2. L'amministratore può preparare la configurazione desiderata sul proprio dispositivo Android (con ESET Endpoint Security installato) ed esportare queste impostazioni in un file (per ulteriori informazioni, consultare la sezione Importa/esporta impostazioni della presente guida). L'amministratore può condividere il file esportato con gli utenti finali (ad esempio, tramite e-mail) e importare il file in qualsiasi dispositivo su cui è in esecuzione ESET Endpoint Security. Nel momento in cui l'utente apre e accetta il file delle impostazioni ricevuto, importerà automaticamente tutte le impostazioni e attiverà l'applicazione (a condizione che siano state incluse le informazioni sulla licenza). Tutte le impostazioni saranno protette dalla password amministratore.

4.1 Download dal sito Web ESET

Scaricare ESET Endpoint Security eseguendo la scansione del codice QR sottostante attraverso l'utilizzo del proprio dispositivo mobile e di un'app di scansione per codici QR:

In alternativa, è possibile scaricare il file di installazione APK di ESET Endpoint Security dal sito Web ESET:

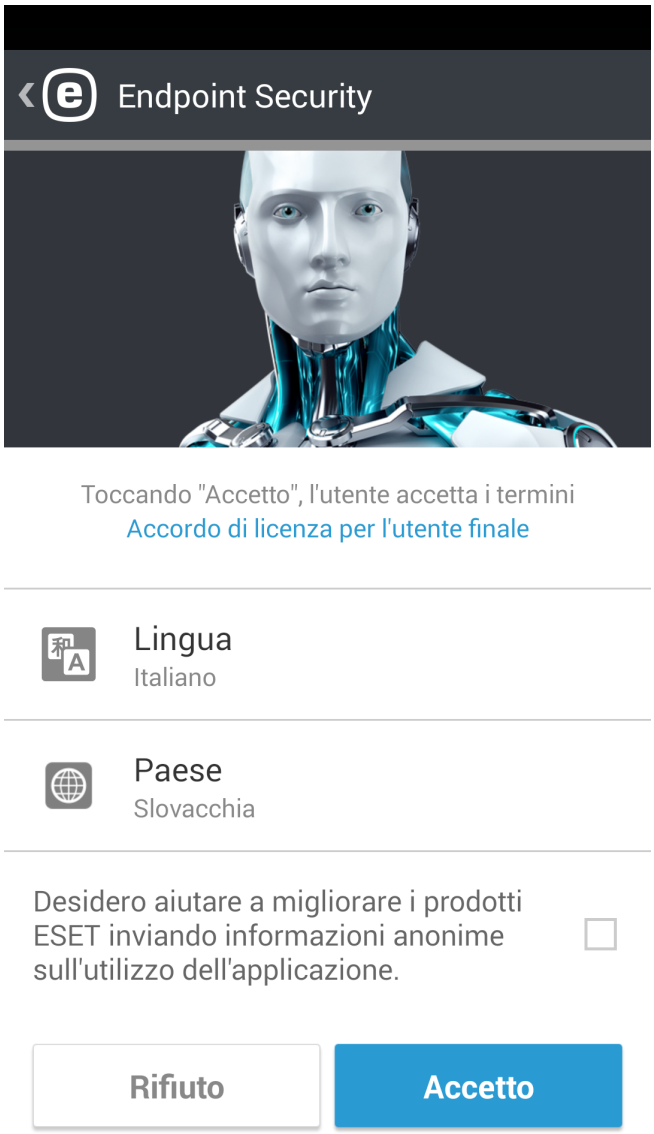
1. Scaricare il file di installazione dal Sito Web ESET.
2. Aprire il file dall'area delle notifiche Android oppure individuarlo utilizzando un'applicazione per la gestione della navigazione dei file. Il file viene salvato solitamente nella cartella Download.
3. Assicurarsi che le applicazioni provenienti da Fonti sconosciute siano consentite sul proprio dispositivo. Per eseguire tale operazione, toccare l'icona dell'utilità di lancio nella schermata iniziale di Android oppure accedere a **Home** > **Menu**. Toccare **Impostazioni** > **Protezione**. L'opzione **Fonti sconosciute** deve essere consentita.
4. Dopo l'apertura del file, toccare **Installa**.

4.2 Download da Google Play

Aprire l'applicazione Google Play Store sul dispositivo Android e ricercare ESET Endpoint Security (oppure solo ESET).

In alternativa, è possibile scaricare il programma eseguendo la scansione del codice QR sottostante attraverso l'utilizzo del dispositivo mobile e di un'app di scansione per codici QR:

4.3 Configurazione guidata



Dopo aver installato l'applicazione, toccare **Configurazione amministratore** e seguire i passaggi della configurazione guidata. Questa procedura è pensata esclusivamente per gli amministratori:

1. Selezionare la **Lingua** che si desidera utilizzare in ESET Endpoint Security.
2. Selezionare il **Paese** in cui ha sede l'attività lavorativa o in cui si risiede.
3. Se si desidera aiutare a migliorare i prodotti ESET inviando informazioni anonime sull'utilizzo dell'applicazione, selezionare l'opzione appropriata.
4. Toccare **Accetto**. Selezionando questa opzione, l'utente accetta l'Accordo di licenza per l'utente finale.
5. Scegliere se collegare ESET Endpoint Security a ESET Remote Administrator o eseguire una configurazione manuale. Quest'ultima opzione richiede la creazione di una password amministratore e l'attivazione della protezione anti-disinstallazione.
6. Nel passaggio successivo, scegliere se si desidera partecipare a ESET Live Grid. Per ulteriori informazioni su ESET Live Grid, consultare questa sezione.
7. Scegliere se si desidera che ESET Endpoint Security rilevi applicazioni potenzialmente indesiderate. Per ulteriori informazioni su queste applicazioni, consultare questa sezione.
8. Attivazione del prodotto.

5. Disinstallazione

ESET Endpoint Security può essere disinstallato utilizzando la procedura guidata Disinstalla disponibile nel menu principale del programma sotto a **Impostazioni** > **Disinstalla**. In caso di disattivazione della protezione anti-disinstallazione, all'utente verrà richiesto di inserire la password amministratore.

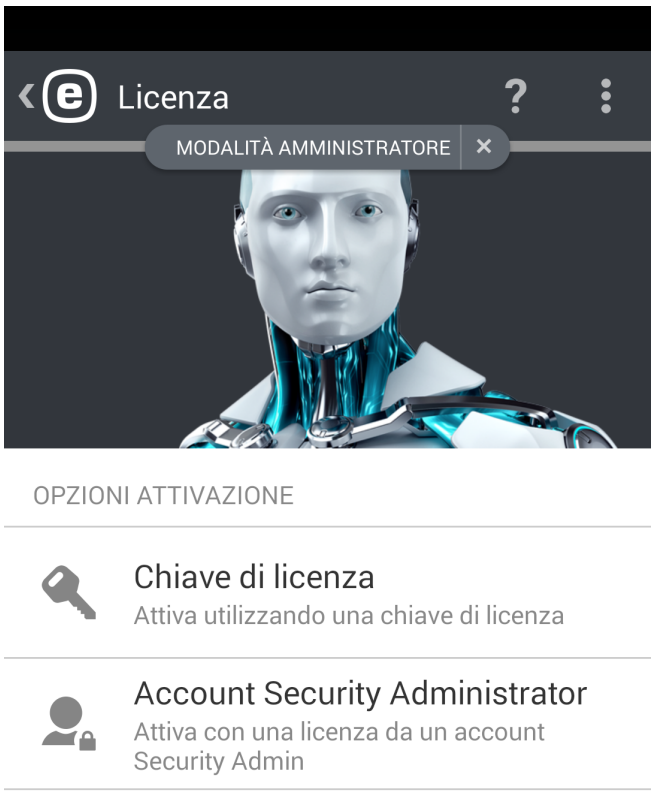
In alternativa, è possibile disinstallare il prodotto manualmente seguendo la procedura sottostante:

1. Toccare l'icona dell'utilità di avvio sulla pagina iniziale di Android (oppure accedere a **Home** > **Menu**) e toccare **Impostazioni** > **Protezione** > **Amministratori del dispositivo**. Deselezionare ESET Endpoint Security e toccare **Disattiva**. Toccare **Sblocca** e inserire la password amministratore. Se ESET Endpoint Security non è stato impostato come amministratore del dispositivo, saltare questo passaggio.
2. Tornare a **Impostazioni** e toccare **Gestisci app** > ESET Endpoint Security > **Disinstalla**.

6. Attivazione prodotto

Esistono vari modi per attivare ESET Endpoint Security. La disponibilità di uno specifico metodo di attivazione varia in base al paese, nonché ai mezzi di distribuzione (pagina Web ESET, ecc.) di un prodotto.

Per attivare ESET Endpoint Security direttamente sul dispositivo Android, toccare l'icona **Menu** nella schermata principale di ESET Endpoint Security (oppure premere il pulsante **MENU** sul dispositivo) e **Licenza**.



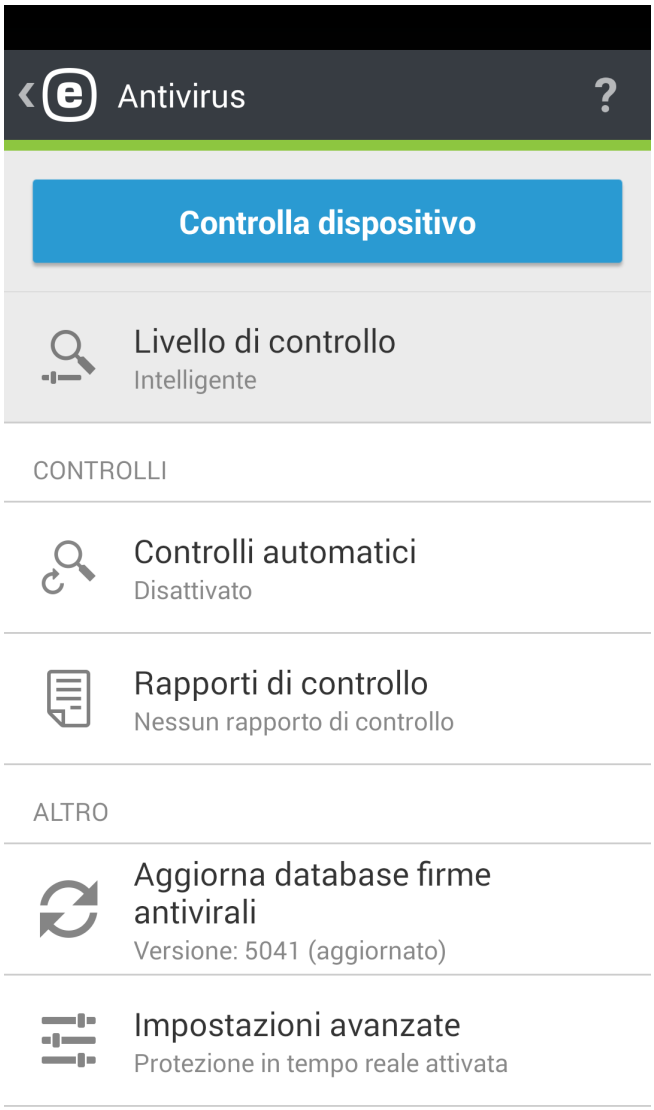
Per attivare ESET Endpoint Security, è inoltre possibile utilizzare uno dei seguenti metodi:

- **Chiave di licenza**: stringa univoca nel formato XXXX-XXXX-XXXX-XXXX-XXXX utilizzata per l'identificazione del proprietario della licenza e per l'attivazione della licenza.
- **Account Security Administrator**: account creato sul portale ESET License Administrator con le credenziali (indirizzo e-mail e password). Questo metodo consente all'utente di gestire licenze multiple da un'unica posizione.

NOTA: ESET Remote Administrator è in grado di attivare i dispositivi client in modo silenzioso attraverso l'utilizzo delle licenze rese disponibili dall'amministratore.

7. Antivirus

Il modulo antivirus protegge il dispositivo dell'utente da codice dannoso bloccando, pulendo o mettendo in quarantena le minacce.



Controlla dispositivo

L'opzione Controlla dispositivo può essere utilizzata per ricercare infiltrazioni nel dispositivo dell'utente.

Alcuni tipi di file predefiniti vengono controllati per impostazione predefinita. Un controllo completo del dispositivo consente di controllare la memoria, i processi in esecuzione e le librerie a collegamento dinamico dipendenti, nonché i file appartenenti ai supporti di archiviazione interni e rimovibili. Un breve riepilogo del controllo verrà salvato in un file di rapporto disponibile nella sezione Rapporti del controllo.

Se si desidera interrompere un controllo già in esecuzione, toccare l'icona .

Livello di controllo

Sono disponibili 2 diversi livelli di controllo tra cui poter scegliere:

- **Intelligente:** il Controllo intelligente eseguirà il controllo delle applicazioni installate, dei file DEX (file eseguibili per il sistema operativo Android), dei file SO (librerie), dei file ZIP con una profondità massima di controllo di 3 archivi nidificati e del contenuto della scheda SD.
- **Approfondito**: verranno controllati tutti i tipi di file indipendentemente dalla relativa estensione sia nella memoria interna, sia nella scheda SD.

Controlli automatici

Oltre al Controllo su richiesta, ESET Endpoint Security offre anche controlli automatici. Per ulteriori informazioni sulle modalità di utilizzo del Controllo durante il caricamento e del Controllo pianificato, leggere questa sezione.

Rapporti del controllo

La sezione Rapporti del controllo contiene dati completi sui controlli completati sotto forma di file di rapporto. Per ulteriori informazioni, consultare la sezione Rapporti dei controlli antivirus del presente documento.

Aggiorna database firme antivirali

Per impostazione predefinita, ESET Endpoint Security prevede un'attività di aggiornamento in grado di garantire un aggiornamento periodico del programma. Per eseguire l'aggiornamento manualmente, toccare **Aggiorna database delle firme antivirali**.

NOTA: per impedire un utilizzo non necessario della larghezza di banda, gli aggiornamenti vengono rilasciati in base alle specifiche necessità in caso di aggiunta di una nuova minaccia. Gli aggiornamenti sono gratuiti se la licenza è attiva, mentre per il servizio di trasferimento dati i provider di servizi mobili potrebbero addebitare costi specifici.

Ulteriori informazioni sulle impostazioni antivirus avanzate sono disponibili nella sezione Impostazioni avanzate del presente documento.

7.1 Controlli automatici

Livello di controllo

Sono disponibili 2 diversi livelli di controllo tra cui poter scegliere. Questa impostazione vale sia per il Controllo durante il caricamento sia per il Controllo pianificato:

- **Intelligente:** il Controllo intelligente eseguirà il controllo delle applicazioni installate, dei file DEX (file eseguibili per il sistema operativo Android), dei file SO (librerie), dei file ZIP con una profondità massima di controllo di 3 archivi nidificati e del contenuto della schedaSD.
- **Approfondito**: verranno controllati tutti i tipi di file indipendentemente dalla relativa estensione sia nella memoria interna, sia nella scheda SD.

Controllo durante il caricamento

Selezionando questa opzione, il controllo si avvierà automaticamente se il dispositivo si trova nello stato inattivo (completamente carico e collegato a un caricatore).

Controllo pianificato

Il Controllo pianificato consente all'utente di eseguire un controllo automatico dei dispositivi a un orario predefinito. Per pianificare un controllo, toccare  accanto a **Controllo pianificato** e specificare la data e l'ora di avvio del controllo. Per impostazione predefinita, è selezionato il valore lunedì alle ore 4:00.

7.2 Rapporti del controllo

I rapporti del controllo vengono creati in seguito a ciascun controllo pianificato o controllo del dispositivo attivato manualmente.

Ciascun rapporto contiene:

- data e ora dell'evento
- durata del controllo
- numero di file controllati
- risultato del controllo o errori riscontrati durante il controllo

7.3 Impostazioni avanzate

Protezione in tempo reale

Questa opzione consente all'utente di attivare/disattivare il controllo in tempo reale. Questo controllo viene lanciato automaticamente all'avvio del sistema e consente di controllare i file con i quali l'utente interagisce. Il programma controlla automaticamente la cartella Download, i file di installazione APK e tutti i file presenti nella scheda SD in seguito all'installazione.

ESET Live Grid

Sviluppato sul sistema avanzato di allarme immediato ThreatSense.Net, ESET Live Grid è progettato per offrire livelli aggiuntivi di protezione ai dispositivi. Controlla continuamente i programmi e i processi in esecuzione sul sistema in base alle informazioni più aggiornate raccolte tra milioni di utenti ESET in tutto il mondo. I controlli sono inoltre elaborati in maniera più rapida e precisa grazie all'ampliamento continuo del database ESET Live Grid. In questo modo è possibile garantire una migliore protezione proattiva e una maggiore velocità di controllo a tutti gli utenti ESET. Si consiglia di attivare questa funzionalità. Grazie per la fiducia accordata.

Rileva applicazioni potenzialmente indesiderate

Un'applicazione indesiderata è un programma che contiene adware, installa barre degli strumenti, tiene traccia dei risultati di ricerca o si prefigge altri obiettivi poco chiari. Esistono alcune situazioni in cui un utente potrebbe percepire che i vantaggi di un'applicazione indesiderata superano i rischi. Per questo motivo, ESET assegna a tali applicazioni una categoria a rischio ridotto rispetto ad altri tipi di software dannosi.

Rileva applicazioni potenzialmente pericolose

Esistono molte applicazioni legali utili per semplificare l'amministrazione dei dispositivi in rete. Tuttavia, nelle mani sbagliate, questi strumenti possono essere utilizzati per scopi illegittimi. L'opzione Rileva applicazioni potenzialmente pericolose consente all'utente di monitorare questi tipi di applicazioni e di bloccarli in base alle sue preferenze. *Applicazioni potenzialmente pericolose* è la classificazione utilizzata per il software legale e commerciale. Questa classificazione include programmi, tra cui strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging.

Blocca minacce non risolte

Questa impostazione determina l'azione che verrà eseguita al termine del controllo e in seguito al rilevamento delle minacce. Attivando questa opzione, il file infetto non sarà eseguibile.

Aggiornamenti database firme antivirali

Questa opzione consente all'utente di impostare l'intervallo temporale in cui gli aggiornamenti del database delle minacce vengono scaricati automaticamente. Questi aggiornamenti vengono rilasciati in base alle specifiche esigenze, nel momento in cui una nuova minaccia viene aggiunta al database. Si consiglia di lasciare impostato il valore predefinito (ogni giorno).

Età massima personalizzata database

Per impostazione predefinita, ESET Endpoint Security sostituisce il database delle firme antivirali ogni 7 giorni in assenza di nuovi aggiornamenti.

Server di aggiornamento

Questa opzione consente all'utente di decidere di aggiornare il proprio dispositivo dal **Server pre-rilascio**. Gli aggiornamenti pre-rilascio vengono sottoposti ad approfondite verifiche interne che saranno presto disponibili per tutti. Gli aggiornamenti pre-rilascio consentono di accedere ai metodi di rilevamento e alle correzioni più recenti. Tuttavia, può accadere che questi strumenti non presentino sempre un livello di stabilità sufficiente. L'elenco di moduli correnti è disponibile nella sezione **Informazioni su**: toccare l'icona del Menu  nella schermata principale di ESET Endpoint Security, quindi **Informazioni su** > ESET Endpoint Security. È consigliabile lasciare attivata l'opzione **Server di rilascio** selezionata per impostazione predefinita.

ESET Endpoint Security consente all'utente di creare copie dei file di aggiornamento che è possibile utilizzare per aggiornare altri dispositivi presenti nella rete. Utilizzo di un **Mirror locale**: è utile disporre di una copia dei file di aggiornamento nell'ambiente LAN, in quanto in questo modo i file di aggiornamento non devono essere scaricati ripetutamente dal server di aggiornamento del fornitore da ciascun dispositivo mobile. Ulteriori informazioni sulle modalità di configurazione del server mirror attraverso l'utilizzo di prodotti ESET Endpoint for Windows sono disponibili in questo documento.

8. Anti-Furto

La funzione **Anti-Furto** protegge il dispositivo mobile dell'utente da accessi non autorizzati.

In caso di smarrimento o furto del dispositivo e di sostituzione della scheda SIM con un'altra scheda (non attendibile), il dispositivo verrà bloccato automaticamente da ESET Endpoint Security e verrà inviato un SMS di avviso al/i numero/i di telefono definito/i dall'utente. Il messaggio includerà il numero di telefono della scheda SIM attualmente inserita, il codice IMSI (International Mobile Subscriber Identity) e il codice IMEI (International Mobile Equipment Identity) del telefono. Un utente non autorizzato non sarà a conoscenza dell'invio di questo messaggio poiché verrà eliminato automaticamente dai thread di messaggistica del dispositivo. È inoltre possibile richiedere le coordinate GPS del dispositivo mobile smarrito o cancellare da remoto tutti i dati archiviati sul dispositivo.

NOTA: alcune funzioni Anti-Furto (schede SIM attendibili e comandi testuali SMS) non sono disponibili sui tablet che non supportano la funzione di messaggistica.

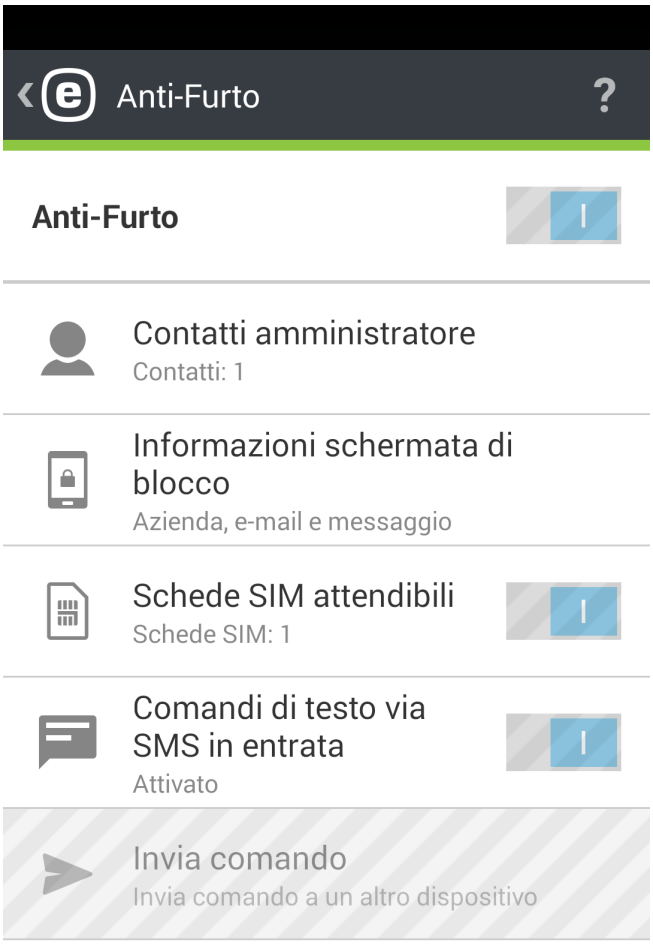
Le funzioni Anti-Furto aiutano gli amministratori a proteggere e a individuare la posizione di un dispositivo mancante. Le azioni possono essere attivate da ERA o tramite i comandi SMS.

ESET Endpoint Security 2 utilizza gli stessi comandi SMS della versione 1 (Blocca, Cancella e Trova). Sono stati aggiunti i seguenti comandi:

- **Sblocca**: sblocca il dispositivo bloccato
- **Ripristino avanzato impostazioni predefinite**: tutti i dati accessibili sul dispositivo verranno rimossi velocemente (le intestazioni dei file verranno distrutte) e sul dispositivo verranno ripristinate le impostazioni predefinite
- **Sirena**: il dispositivo smarrito verrà bloccato e verrà emesso un suono molto acuto anche in modalità silenziosa

Per potenziare il livello di sicurezza dei comandi SMS, l'amministratore riceverà un codice SMS di verifica univoco e con un periodo di validità limitato sul proprio telefono cellulare (al numero definito nell'elenco di contatti dell'amministratore) durante l'esecuzione di un comando SMS. Questo codice di verifica verrà utilizzato per la verifica di un comando specifico.

Ad esempio, se un amministratore invia un SMS a un dispositivo gestito (ad esempio, un telefono cellulare smarrito) contenente il testo *eset lock,* riceverà un SMS contenente un codice di verifica per quel comando. L'amministratore invia quindi un nuovo SMS allo stesso numero di cellulare contenente il testo *blocco eset* seguito dal codice di conferma. Dopo questi passaggi, il comando verrà verificato ed eseguito. I comandi SMS possono essere inviati da qualsiasi telefono cellulare e numero di dispositivo mobile presente tra i contatti dell'amministratore.



Durante l'esecuzione di comandi tramite SMS, l'amministratore riceve un SMS di conferma dell'invio di uno specifico comando. Durante l'esecuzione dei comandi da ERA, l'amministratore riceve una conferma in ERA.

Durante la ricezione di informazioni sulla posizione (comando Trova), l'amministratore che utilizza ESET Remote Administrator riceve le informazioni sulla posizione sotto forma di coordinate GPS. Durante l'esecuzione del comando tramite SMS, le informazioni sulla posizione (coordinate GPS e un collegamento a Google Maps) vengono ricevute tramite SMS. Durante l'utilizzo della GUI per i comandi SMS (funzione **Invia comando**), le informazioni ricevute vengono presentate nella GUI dedicata.

Tutti i comandi Anti-Furto possono essere eseguiti anche da ERA. Una nuova funzionalità per la gestione dei dispositivi mobili consente agli amministratori di eseguire comandi Anti-Furto in pochi semplici clic. Le attività vengono inviate immediatamente per l'esecuzione attraverso un nuovo componente di elaborazione dei comandi push (connettore di dispositivi mobili) che è ora parte dell'infrastruttura ERA.

8.1 Contatti amministratore

Elenco dei numeri di telefono dell'amministratore protetti dalla password amministratore. I comandi Anti-Furto possono essere inviati solo da numeri attendibili. Questi numeri vengono utilizzati anche per le notifiche correlate alle azioni Anti-Furto.

8.1.1 Come aggiungere un contatto dell'amministratore

Durante la configurazione guidata della funzione Anti-Furto, dovrebbero essere stati inseriti il nome e il numero di telefono dell'amministratore. Se il contatto contiene più di un numero di telefono, verranno presi in considerazione tutti i numeri associati.

I contatti dell'amministratore possono essere aggiunti o modificati nella sezione **Anti-Furto** > **Contatti amministratore**.

8.2 Informazioni sulla schermata di blocco

L'amministratore è in grado di definire informazioni personalizzate (ragione sociale, indirizzo di posta elettronica, messaggio) che verranno visualizzate quando il dispositivo è bloccato, con la possibilità di chiamare uno dei contatti amministratore predefiniti.

Queste informazioni includono:

- Ragione sociale (facoltativo)
- Indirizzo e-mail (facoltativo)
- Un messaggio personalizzato

8.3 Schede SIM attendibili

La sezione **SIM attendibile** consente di visualizzare l'elenco di schede SIM attendibili che verranno accettate da ESET Endpoint Security. Se si inserisce una scheda SIM non definita nell'elenco, la schermata verrà bloccata e all'amministratore verrà inviato un SMS di avviso.

Per aggiungere una nuova scheda SIM, toccare l'icona ➕. Inserire un **Nome** per la scheda SIM (ad esempio, Casa, Lavoro) e il relativo numero IMSI (International Mobile Subscriber Identity). Il numero IMSI si presenta generalmente sotto forma di una serie di 15 cifre stampate sulla scheda SIM dell'utente. In alcuni casi, la stringa può anche essere più corta.

Per rimuovere una scheda SIM dall'elenco, toccare e tenere premuta la voce, quindi toccare l'icona 🗑.

NOTA: la funzione SIM attendibile non è disponibile su dispositivi CDMA, WCDMA e sui dispositivi su cui è attiva solo una connessione Wi-Fi.

8.4 Comandi remoti

I comandi remoti possono essere attivati in tre modi:

- direttamente dalla console ERA
- utilizzando la funzione **Invia comando** in ESET Endpoint Security installata sul dispositivo Android dell'amministratore
- inviando messaggi di testo SMS dal dispositivo dell'amministratore

Per facilitare l'esecuzione dei comandi SMS per un amministratore che non utilizza ERA, è possibile effettuarne l'attivazione da ESET Endpoint Security installato sul dispositivo Android dell'amministratore. Anziché digitare manualmente il messaggio di testo e verificare il comando con il codice di verifica, l'amministratore può utilizzare la funzione **Invia comando**(disponibile solo in modalità amministratore). Un amministratore può inserire il numero di telefono o scegliere un contatto e selezionare il comando dal menu a discesa. ESET Endpoint Security eseguirà automaticamente tutti i passaggi necessari in modalità silenziosa in background.

Quando si inviano comandi SMS, il numero di telefono di un amministratore deve essere un Contatto amministratore sul dispositivo di destinazione. L'amministratore riceverà un codice di notifica valido per un'ora che può essere utilizzato per eseguire uno dei comandi elencati di seguito. Il codice deve essere allegato al messaggio con cui viene inviato il comando nel seguente formato: `codiceeset find`. L'amministratore riceverà una conferma quando il comando è stato eseguito sul dispositivo di destinazione. Possono essere inviati i seguenti comandi SMS:

Trova
Comando SMS: `eset find`
L'utente riceverà un messaggio di testo contenente le coordinate GPS del dispositivo di destinazione, con un collegamento alla posizione specifica sulle mappe Google. Se dopo 10 minuti è disponibile una posizione più precisa, il dispositivo invierà un nuovo SMS.

Blocca
Comando SMS: `eset lock`
Il dispositivo verrà bloccato. L'utente potrà sbloccarlo utilizzando la password amministratore o il comando remoto di sblocco. Quando si invia questo comando tramite SMS, è possibile allegare un messaggio personalizzato che sarà visualizzato sullo schermo del dispositivo bloccato. Usare il seguente formato: `messaggio codiceeset lock`. Se si lascia vuoto il parametro del messaggio, verrà visualizzata una sezione Informazioni sulla schermata di blocco del messaggio.

Sblocca
Comando SMS: `eset unlock`
Il dispositivo verrà sbloccato e la scheda SIM attualmente nel dispositivo verrà salvata come SIM attendibile.

Sirena
Comando SMS: `eset siren`
La sirena ad alto volume si attiverà anche se il dispositivo è impostato su silenzioso.

Ripristino avanzato impostazioni predefinite
Comando SMS: `eset enhanced factory reset`
Questa opzione ripristinerà le impostazioni predefinite del dispositivo. Tutti i dati accessibili verranno cancellati e le intestazioni dei file rimosse. L''operazione potrebbe richiedere alcuni minuti.

Cancella
Comando SMS: `eset wipe`
Tutti i contatti, i messaggi, le e-mail, gli account, i contenuti della scheda SD, le immagini, la musica e i video archiviati nelle cartelle predefinite verranno eliminati in modo permanente dal dispositivo. ESET Endpoint Security rimarrà installato sul dispositivo.

NOTA: i comandi SMS non fanno distinzione tra lettera maiuscola e minuscola.

9. Controllo applicazione

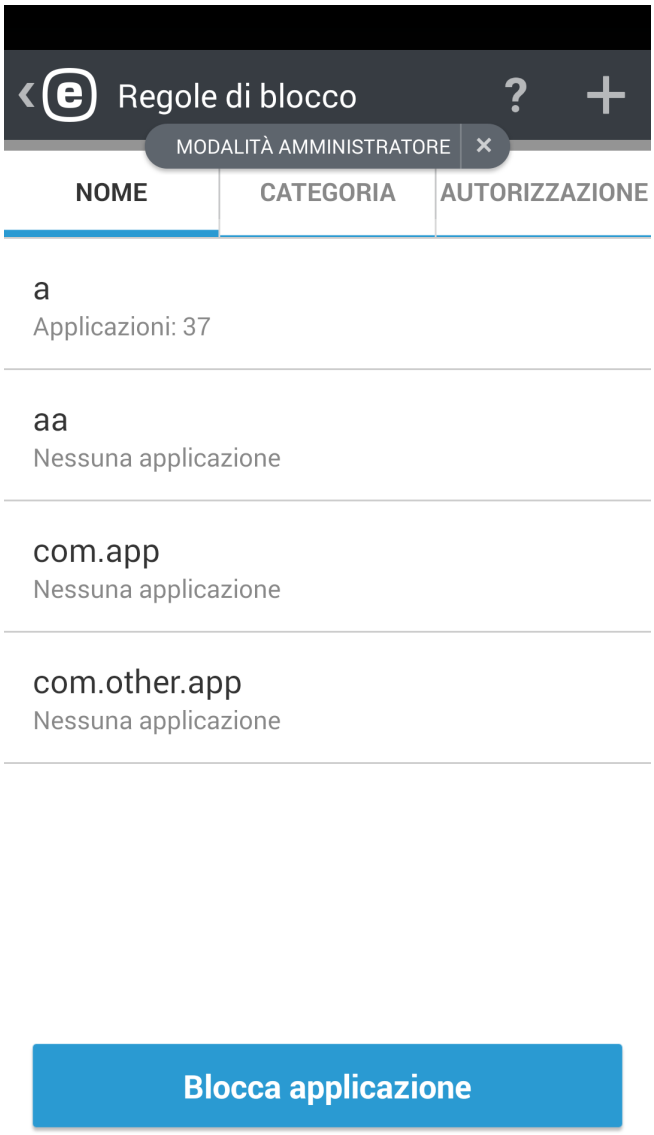
La funzione **Controllo applicazione** consente agli amministratori di monitorare le applicazioni installate, bloccare l'accesso ad applicazioni definite e ridurre il rischio di esposizione suggerendo agli utenti la disinstallazione di specifiche applicazioni. L'amministratore può selezionare uno dei vari metodi di filtraggio per le applicazioni:

- Definire manualmente le applicazioni da bloccare
- Eseguire un blocco in base alla categoria (ad esempio, giochi o social)
- Eseguire un blocco in base alle autorizzazioni (ad esempio, applicazioni in grado di monitorare il posizionamento)
- Eseguire un blocco in base all'origine (ad esempio, applicazioni installate da fonti diverse da Google Play Store)

9.1 Regole di blocco

Nella sezione **Controllo applicazione** > **Blocco** > **Regole di blocco**, è possibile creare le regole per il blocco dell'applicazione sulla base dei criteri che seguono:

- nome dell'applicazione o nome del pacchetto
- categoria
- autorizzazioni



9.1.1 Blocco in base al nome dell'applicazione

ESET Endpoint Security consente agli amministratori di bloccare l'applicazione in base al nome o al nome del pacchetto. La sezione **Regole di blocco** offre una panoramica delle regole create e un elenco delle applicazioni bloccate.

Per modificare una regola esistente, toccare e tenere premuta la regola, quindi toccare **Modifica** . Per rimuovere voci della regola dall'elenco, toccarle e tenerle premute, selezionare quelle che si desiderano rimuovere, quindi toccare **Rimuovi** . Per cancellare l'intero elenco, toccare **SELEZIONA TUTTO**, quindi toccare **Rimuovi** .

Quando si blocca un'applicazione in base al nome, ESET Endpoint Security ricercherà la corrispondenza esatta con il nome di un'applicazione lanciata. Se si modifica l'interfaccia grafica utente di ESET Endpoint Security su una lingua differente, è necessario reinserire il nome dell'applicazione in tale lingua per continuare a bloccarla.

Per evitare problemi con i nomi delle applicazioni localizzate, è consigliabile bloccare tali applicazioni in base ai nomi dei rispettivi pacchetti, ovvero un identificativo univoco delle applicazioni che non può essere modificato durante l'esecuzione o riutilizzato da un'altra applicazione.

In caso di amministratore locale, un utente può trovare il nome del pacchetto dell'installazione in **Controllo applicazione** > **Monitoraggio** > **Applicazioni consentite**. Dopo aver toccato l'applicazione, nella schermata **Dettaglio** verrà visualizzato il nome del pacchetto dell'applicazione. Per bloccare l'applicazione, attenersi ai passaggi indicati.

9.1.1.1 Come bloccare un'applicazione in base al nome

1. Toccare **Controllo applicazione** > **Blocco** > **Blocca applicazione** > **Blocca per nome**.
2. Scegliere se bloccare l'applicazione in base al nome o al nome del pacchetto.
3. Inserire le parole in base all'applicazione che verrà bloccata. In presenza di più di una parola, utilizzare una virgola (,) come separatore.

Ad esempio, la parola "*poker*" nel campo **Nome dell'applicazione** bloccherà tutte le applicazioni il cui nome contiene "*poker*". Inserendo "*com.poker.game*" nel campo **Nome pacchetto**, ESET Endpoint Security bloccherà solo un'applicazione.

9.1.2 Blocco in base alla categoria dell'applicazione

ESET Endpoint Security consente all'amministratore di bloccare l'applicazione in base a categorie predefinite. La sezione **Regole di blocco** offre all'utente una panoramica delle regole create e un elenco delle applicazioni bloccate.

Se si desidera modificare una regola esistente, toccare e tenere premuta la regola, quindi toccare **Modifica**  .

Per rimuovere una voce della regola dall'elenco, toccarla e tenerla premuta, quindi toccare **Rimuovi**  . Per cancellare l'intero elenco, toccare **SELEZIONA TUTTO**.

9.1.2.1 Come bloccare un'applicazione in base alla categoria

1. Toccare **Controllo applicazione** > **Blocco** > **Blocca applicazione** > **Blocca per categoria**.
2. Selezionare le categorie predefinite utilizzando le caselle di controllo e toccare **Blocca**.

9.1.3 Blocco in base alle autorizzazioni dell'applicazione

ESET Endpoint Security consente all'amministratore di bloccare l'applicazione in base alle relative autorizzazioni. La sezione **Regole di blocco** offre all'utente una panoramica delle regole create e un elenco delle applicazioni bloccate.

Se si desidera modificare una regola esistente, toccare e tenere premuta la regola, quindi toccare **Modifica**  .

Per rimuovere una voce della regola dall'elenco, toccarla e tenerla premuta, quindi toccare **Rimuovi**  . Per cancellare l'intero elenco, toccare **SELEZIONA TUTTO**.

9.1.3.1 Come bloccare un'applicazione in base alle autorizzazioni

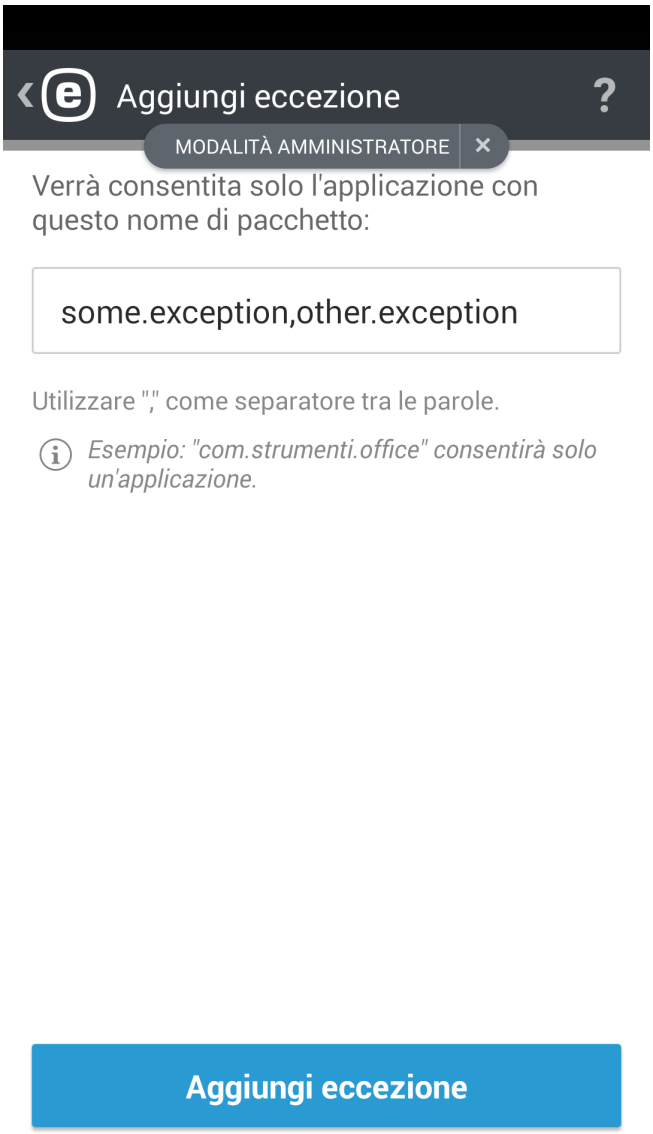
1. Toccare **Controllo applicazione** > **Blocco** > **Blocca applicazione** > **Blocca per autorizzazione**.
2. Selezionare le autorizzazioni utilizzando le caselle di controllo e toccare **Blocca**.

9.1.4 Blocca origini sconosciute

Per impostazione predefinita, ESET Endpoint Security non blocca le applicazioni scaricate da Internet o ottenute da fonti diverse da Google Play Play Store. La sezione **Applicazioni bloccate** offre all'utente una panoramica delle applicazioni bloccate (nome del pacchetto, regola applicata) e la possibilità di disinstallare l'applicazione o aggiungerla alla whitelist nella sezione **Eccezioni**.

9.2 Eccezioni

È possibile creare eccezioni per escludere una specifica applicazione dall'elenco di applicazioni bloccate. Gli amministratori che gestiscono ESET Endpoint Security da remoto possono utilizzare questa nuova funzione per stabilire se un dato dispositivo è conforme o meno alle politiche aziendali in materia di applicazioni installate.

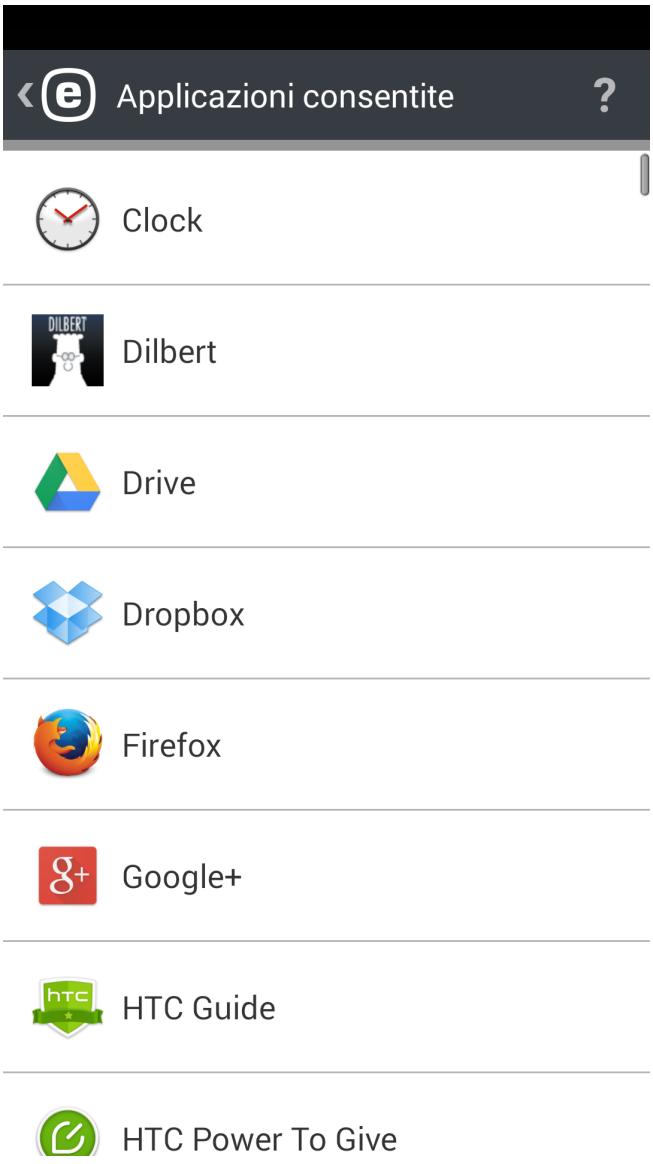


9.2.1 Come aggiungere eccezioni

Oltre ad aggiungere la nuova eccezione (attraverso l'inserimento del nome del pacchetto dell'applicazione), è possibile inserire le applicazioni in una whitelist escludendole dall'elenco di **Applicazioni bloccate**.

9.3 Applicazioni consentite

Questa sezione offre all'utente una panoramica delle applicazioni installate che non sono state bloccate dalle regole. Se si desidera bloccare un'applicazione presente in questa sezione, selezionarla e toccare l'icona del **Menu** nell'angolo in alto a destra della schermata, quindi toccare **Blocca**. L'applicazione verrà spostata nell'elenco di **Applicazioni bloccate** (in **Controllo applicazione** > **Blocco**).

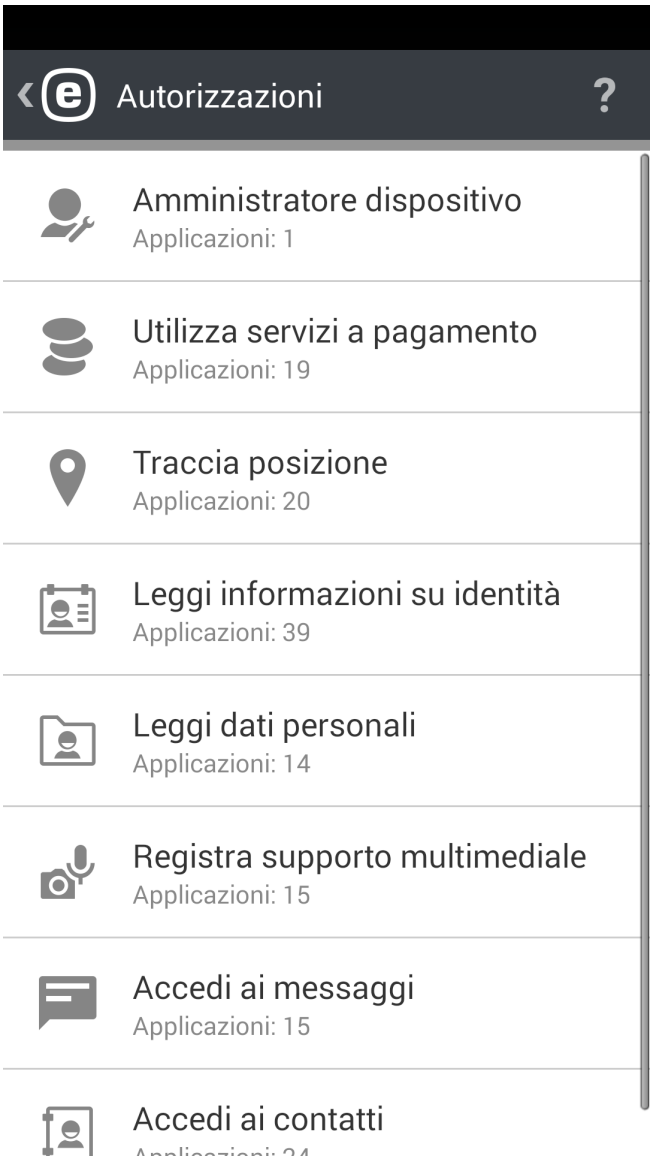


9.4 Autorizzazioni

Questa funzione consente di monitorare il comportamento delle applicazioni che hanno accesso a dati personali o aziendali e offre all'amministratore la possibilità di controllare gli accessi dell'applicazione sulla base di categorie di autorizzazione predefinite.

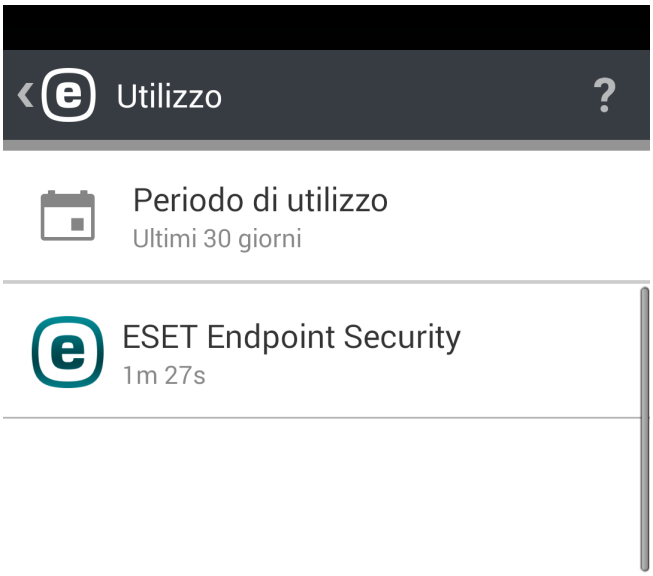
Alcune applicazioni installate sul dispositivo dell'utente potrebbero avere accesso a servizi a pagamento, monitorare la posizione dell'utente o leggere le informazioni personali, i contatti o i messaggi di testo. ESET Endpoint Security offre la possibilità di controllare queste applicazioni.

In questa sezione, è disponibile un elenco di applicazioni ordinate in base alla categoria. Toccare ciascuna categoria per visualizzarne una descrizione dettagliata. Per consultare i dettagli relativi alle autorizzazioni di ciascuna applicazione, toccare l'applicazione di interesse.


Autorizzazioni
?
Amministratore dispositivo
Applicazioni: 1
Utilizza servizi a pagamento
Applicazioni: 19
Traccia posizione
Applicazioni: 20
Leggi informazioni su identità
Applicazioni: 39
Leggi dati personali
Applicazioni: 14
Registra supporto multimediale
Applicazioni: 15
Accedi ai messaggi
Applicazioni: 15
Accedi ai contatti

9.5 Utilizzo

In questa sezione, l'amministratore può monitorare il tempo di utilizzo di specifiche applicazioni da parte di un utente. Per filtrare l'elenco di applicazioni in base al periodo di utilizzo, utilizzare l'opzione **Periodo di utilizzo** e scegliere se visualizzare le applicazioni utilizzate negli ultimi 30 giorni, 7 giorni o 24 ore.

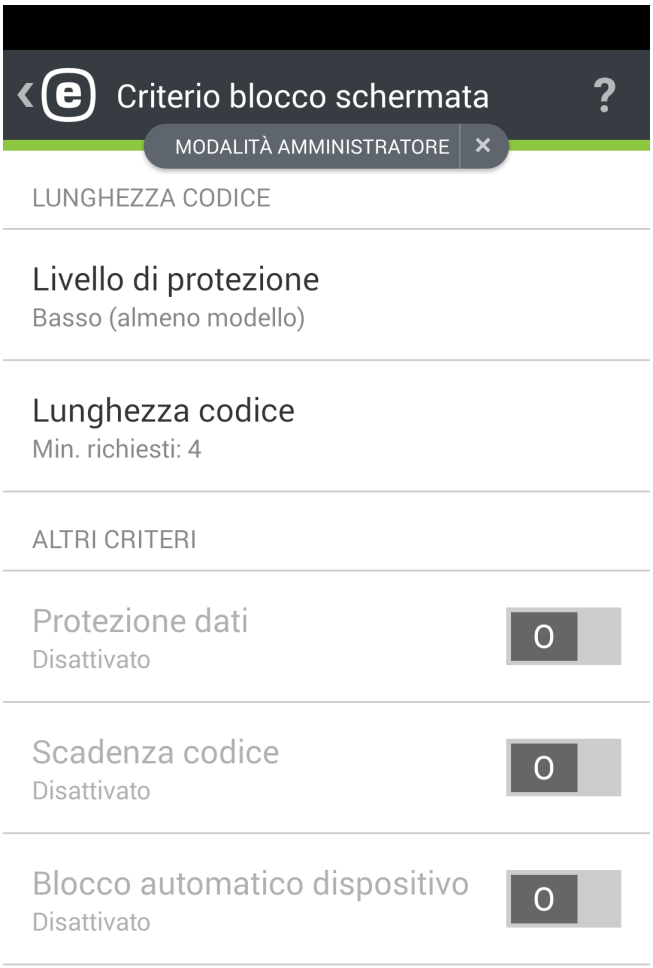


10. Protezione dispositivo

La **Protezione dispositivo** offre agli amministratori la possibilità di eseguire le seguenti azioni:

- eseguire criteri di protezione di base sui dispositivi mobili e definire criteri per impostazioni importanti del dispositivo
- specificare la lunghezza richiesta del codice di blocco della schermata
- limitare l'utilizzo della fotocamera integrata

10.1 Criterio di blocco della schermata



In questa sezione, l'amministratore potrà:

- impostare un livello minimo di protezione (modello, PIN, password) per il codice di blocco della schermata del sistema e definire la complessità del codice (ad esempio, lunghezza minima del codice)
- impostare il numero massimo di tentativi di sblocco non riusciti (in alternativa, sul dispositivo verranno ripristinate le impostazioni predefinite)
- impostare la validità massima del codice di blocco della schermata
- impostare il timer per il blocco della schermata

ESET Endpoint Security invia una notifica automatica all'utente e all'amministratore se le impostazioni correnti del dispositivo sono conformi alle politiche aziendali in materia di sicurezza. Se un dispositivo non è conforme, l'applicazione suggerirà automaticamente all'utente le modifiche da applicare per renderlo nuovamente conforme.

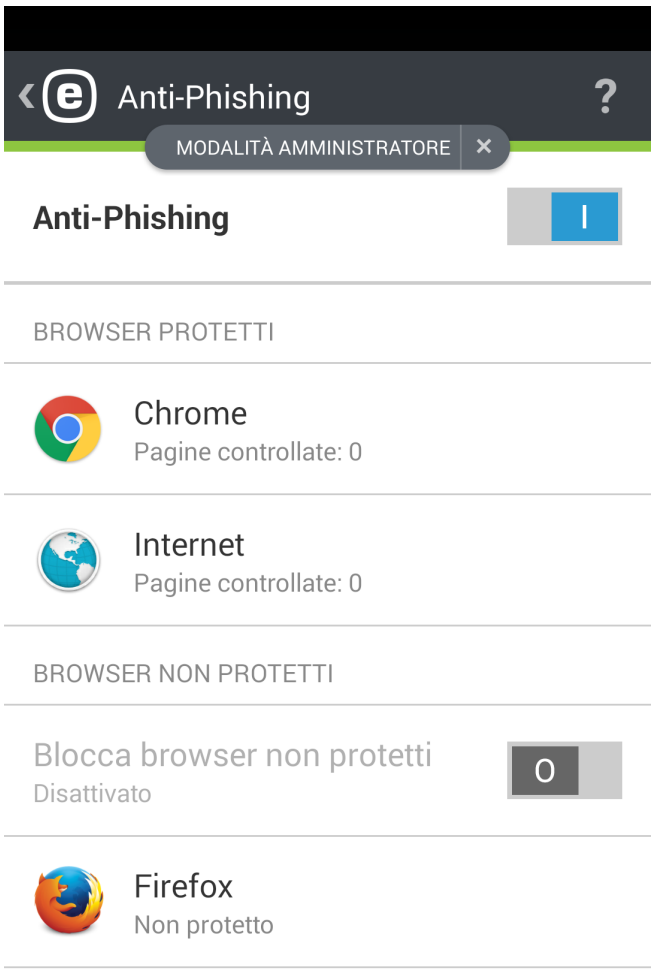
10.2 Criterio impostazioni dispositivo

La Protezione dispositivo include anche il **Criterio impostazioni dispositivo** (precedentemente parte della funzionalità Controllo di protezione) che offre all'amministratore del sistema la possibilità di monitorare le impostazioni predefinite del dispositivo per stabilire se siano state o meno impostate quelle consigliate.

Le impostazioni del dispositivo includono:

- Wi-Fi
- Satelliti GPS
- Servizi di posizionamento
- Memoria
- Roaming dati
- Roaming chiamate
- Origini sconosciute
- Modalità debug
- NFC
- Crittografia archiviazione
- Dispositivo con radice

11. Anti-Phishing



Il termine *phishing* definisce un'attività illegale che si avvale dell'ingegneria sociale, manipolando gli utenti al fine di ottenere informazioni riservate. Il phishing viene utilizzato solitamente per ottenere l'accesso a dati sensibili, tra cui numeri di conti bancari, numeri di carte di credito, codici PIN o nomi utenti e password.

Si consiglia di lasciare attivata l'opzione **Anti-Phishing**. Tutti gli attacchi phishing potenziali provenienti da siti Web o domini presenti nel database dei malware ESET verranno bloccati e verrà visualizzata una notifica di avviso che fornisce all'utente informazioni relative all'attacco.

La funzione Anti-Phishing integra i browser Web più comuni disponibili sul sistema operativo Android (ad esempio, Chrome e il browser Web predefinito Android). L'accesso ad altri browser che verranno indicati come non protetti può essere bloccato facendo clic sul pulsante  .

Per utilizzare tutte le funzionalità offerte dall'Anti-Phishing, si consiglia di bloccare tutti i browser Web non supportati, in modo da consentire agli utenti di utilizzare esclusivamente i browser supportati.

NOTA: la funzione Anti-Phishing offre protezione durante la navigazione in modalità privata (incognito).

12. Filtro SMS e chiamate

Il **Filtro SMS e chiamate** blocca i messaggi SMS/MMS in entrata e le chiamate in entrata/in uscita in base alle regole definite dall'utente.

I messaggi non desiderati includono solitamente annunci pubblicitari provenienti da provider di servizi di telefonia mobile o messaggi di utenti sconosciuti o non specificati. L'espressione "blocca messaggio" fa riferimento allo spostamento automatico di un messaggio in entrata nella sezione **Cronologia**. In caso di blocco di un messaggio o di una chiamata in entrata, non viene visualizzata alcuna notifica. Il vantaggio di tale funzione consiste nel fatto che l'utente non verrà disturbato da informazioni non richieste, ma potrà sempre controllare i rapporti dei messaggi bloccati per errore.

NOTA: il filtro SMS e chiamate non funziona sui tablet che non supportano i servizi di chiamata e di messaggistica. Il filtraggio SMS/MMS non è disponibile sui dispositivi Android OS 4.4 (KitKat) e sarà disattivato sui dispositivi sui quali Google Hangouts è impostato come applicazione principale per gli SMS.

Per bloccare le chiamate e i messaggi provenienti dall'ultimo numero ricevuto, toccare **Blocca ultimo chiamante** o **Blocca ultimo mittente SMS**. Questa opzione consentirà di creare una nuova regola.

12.1 Regole

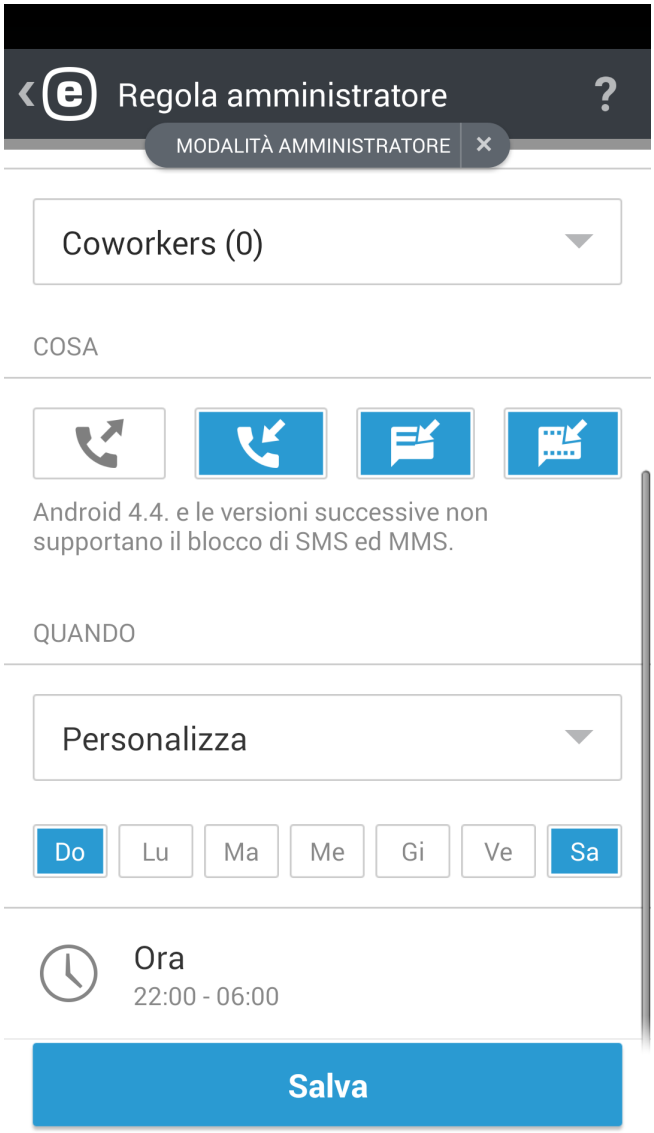
Un utente può creare regole senza la necessità di inserire una password amministratore. Le regole dell'amministratore possono essere create solo in modalità amministratore. Le regole dell'amministratore sovrascriveranno le eventuali regole dell'utente.

Per ulteriori informazioni sulla creazione di una nuova regola, consultare questa sezione.

Se si desidera rimuovere la voce di una regola esistente dall'elenco **Regole**, toccarla e tenerla premuta, quindi toccare l'icona **Rimuovi**  .

12.1.1 Come aggiungere una nuova regola

Per aggiungere una nuova regola, toccare l'icona ✚ nell'angolo in alto a destra della schermata **Regole**.



In base all'azione che si desidera far eseguire alla regola, scegliere se i messaggi e le chiamate verranno consentiti o bloccati.

Specificare una persona o un gruppo di numeri di telefono. ESET Endpoint Security riconoscerà i gruppi di contatti salvati in Contatti (ad esempio, Famiglia, Amici o Colleghi). **Tutti i numeri sconosciuti** includerà i numeri di telefono non salvati nell'elenco dei contatti. È possibile utilizzare questa opzione per bloccare chiamate telefoniche non gradite (ad esempio, telefonate non richieste) oppure per impedire ai dipendenti di un'azienda di comporre numeri sconosciuti. L'opzione **Tutti i numeri noti** fa riferimento a tutti i numeri di telefono salvati nell'elenco dei contatti. L'opzione **Numeri nascosti** verrà applicata agli ID chiamanti che hanno nascosto intenzionalmente il proprio numero di telefono attraverso la funzione Calling Line Identification Restriction (CLIR).

Specificare i numeri da bloccare o consentire:

- chiamate in uscita
- chiamate in entrata
- messaggi di testo in entrata (SMS) o
- messaggi multimediali in entrata (MMS)

Per applicare la regola esclusivamente per uno specifico periodo di tempo, toccare **Sempre** > **Personalizzato** e selezionare i giorni della settimana e un intervallo temporale nel quale si desidera applicare la regola. Per impostazione predefinita, sono selezionati i giorni sabato e domenica. Questa funzionalità si rivela utile nel caso in cui l'utente desideri non essere disturbato nel corso di riunioni, viaggi di lavoro, di notte o durante il weekend.

NOTA: se l'utente si trova all'estero, tutti i numeri di telefono inseriti nell'elenco devono includere il prefisso internazionale seguito dal numero effettivo (ad esempio, +1610100100).

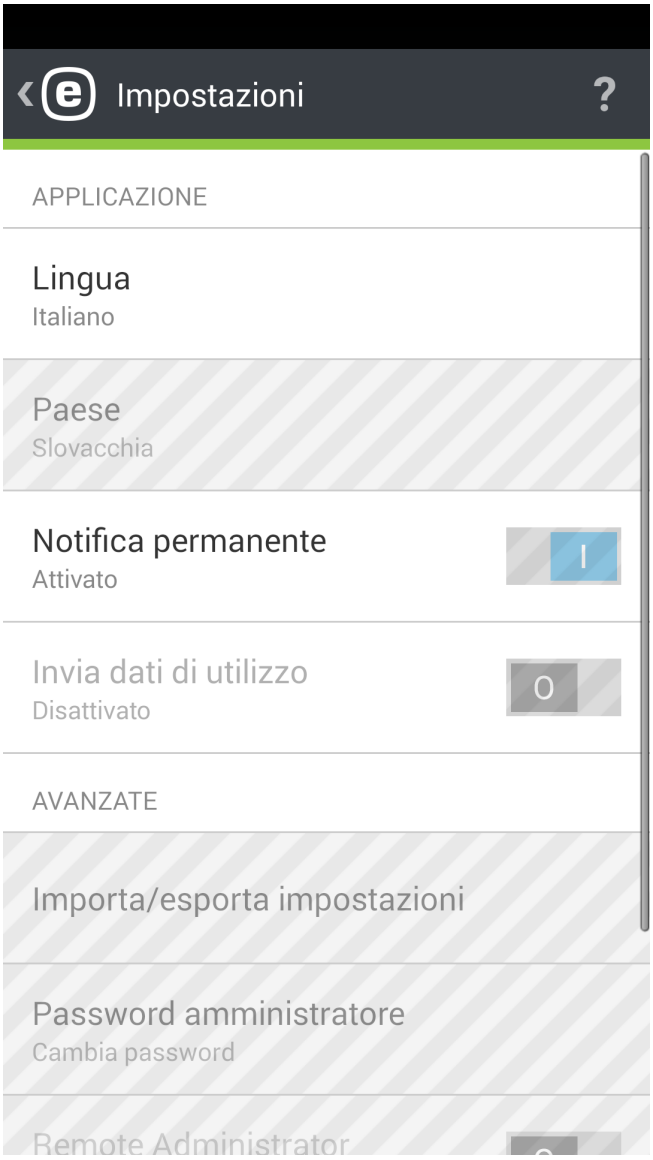
12.2 Cronologia

Nella sezione **Cronologia**, è possibile visualizzare le chiamate e i messaggi bloccati o consentiti dal filtro SMS e chiamate. Ciascun rapporto contiene il nome, il numero di telefono, la data e l'ora dell'evento. I rapporti dei messaggi SMS ed MMS contengono anche il corpo dei messaggi.

Se si desidera modificare una regola correlata a un numero di telefono o un contatto bloccato, toccare la voce presente nell'elenco e l'icona .

Per rimuovere la voce dall'elenco, selezionarla e toccare l'icona . Per rimuovere voci multiple, toccarle e tenerle premute, quindi toccare l'icona .

13. Impostazioni



Lingua
Per impostazione predefinita, ESET Endpoint Security viene installato nella lingua delle impostazioni internazionali di sistema del dispositivo dell'utente (in Lingua del sistema operativo Android e nelle impostazioni della tastiera). Per modificare la lingua dell'interfaccia utente dell'applicazione, toccare Lingua e selezionare il valore desiderato.

Paese
Selezionare il Paese in cui ha sede l'attività lavorativa o in cui si risiede.

Aggiornamento
Per garantire un livello di protezione massimo, utilizzare l'ultima versione di ESET Endpoint Security. Toccare **Aggiorna** per verificare la disponibilità di una versione più recente da scaricare dal sito Web ESET. Questa opzione non è disponibile se ESET Endpoint Security è stato scaricato da Google Play. In questo caso, il prodotto viene aggiornato da Google Play.

Notifica permanente

ESET Endpoint Security consente di visualizzare l'icona di notifica nell'angolo in alto a sinistra della schermata (barra di stato Android). Se non si desidera visualizzare l'icona, deselezionare **Notifica permanente**.

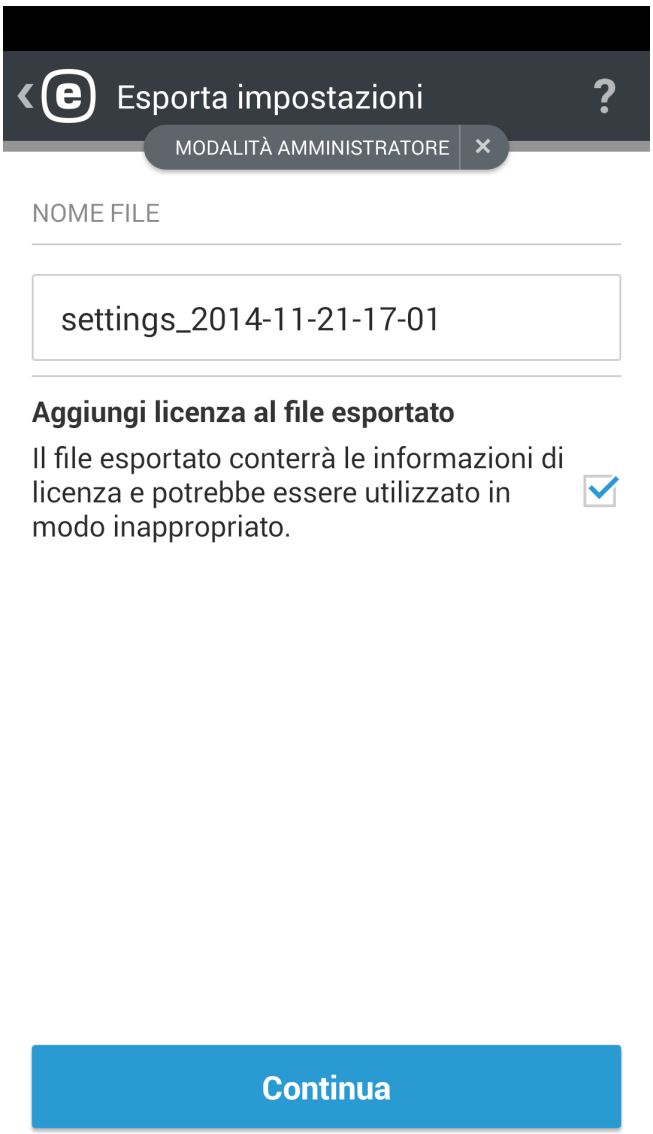
Invia dati di utilizzo
Questa opzione aiuta a migliorare i prodotti ESET attraverso l'invio di informazioni anonime sull'utilizzo dell'applicazione. Se questa opzione non è stata attivata durante la procedura di installazione guidata all'avvio, è possibile farlo nella sezione **Impostazioni**.

Password amministratore
Questa opzione consente all'utente di impostare una nuova password amministratore o di modificare quella esistente. Per ulteriori informazioni, consultare la sezione Password amministratore del presente documento.

Disinstalla
Attraverso l'esecuzione della procedura di disinstallazione, ESET Endpoint Security e le cartelle della quarantena verranno rimossi in modo permanente dal dispositivo. In caso di attivazione della protezione anti-disinstallazione, all'utente verrà richiesto di inserire la **Password amministratore**.

13.1 Importa/esporta impostazioni

Per un'agevole condivisione delle impostazioni tra due dispositivi mobili non gestiti da ERA, ESET Endpoint Security 2 introduce la possibilità di esportare e di importare le impostazioni del programma. L'amministratore può esportare manualmente le impostazioni del dispositivo in un file che è possibile condividere (ad esempio, tramite e-mail) e importare in qualsiasi dispositivo su cui è in esecuzione l'applicazione client. Nel momento in cui l'utente accetta il file delle impostazioni ricevuto, definisce automaticamente tutte le impostazioni e attiva l'applicazione (a condizione che siano state incluse le informazioni sulla licenza). Tutte le impostazioni saranno protette dalla password amministratore.



13.1.1 Esporta impostazioni

Per esportare le impostazioni correnti di ESET Endpoint Security, specificare il nome del file delle impostazioni: i campi della data e dell'ora correnti verranno completati automaticamente. È inoltre possibile aggiungere le informazioni sulla licenza (chiave di licenza o indirizzo e-mail e password dell'account Security Admin) nel file esportato. Tuttavia, è necessario tenere presente che queste informazioni non saranno crittografate e potrebbero essere utilizzate per scopi illegittimi.

Nel passaggio successivo, selezionare le modalità di condivisione del file attraverso:

- la rete Wi-Fi
- il Bluetooth
- l'e-mail
- Gmail
- l'applicazione utilizzata per la navigazione dei file (ad esempio, ASTRO File Manager o ES File Explorer)

13.1.2 Importa impostazioni

Per importare le impostazioni da un file posizionato sul dispositivo, utilizzare un'applicazione per la navigazione dei file, come ad esempio ASTRO File Manager o ES File Explorer, individuare il file delle impostazioni e scegliere ESET Endpoint Security.

Le impostazioni possono essere importate anche selezionando un file nella sezione **Cronologia**.

13.1.3 Cronologia

La sezione **Cronologia** offre all'utente l'elenco dei file delle impostazioni importate che possono essere così condivisi, importati e rimossi.

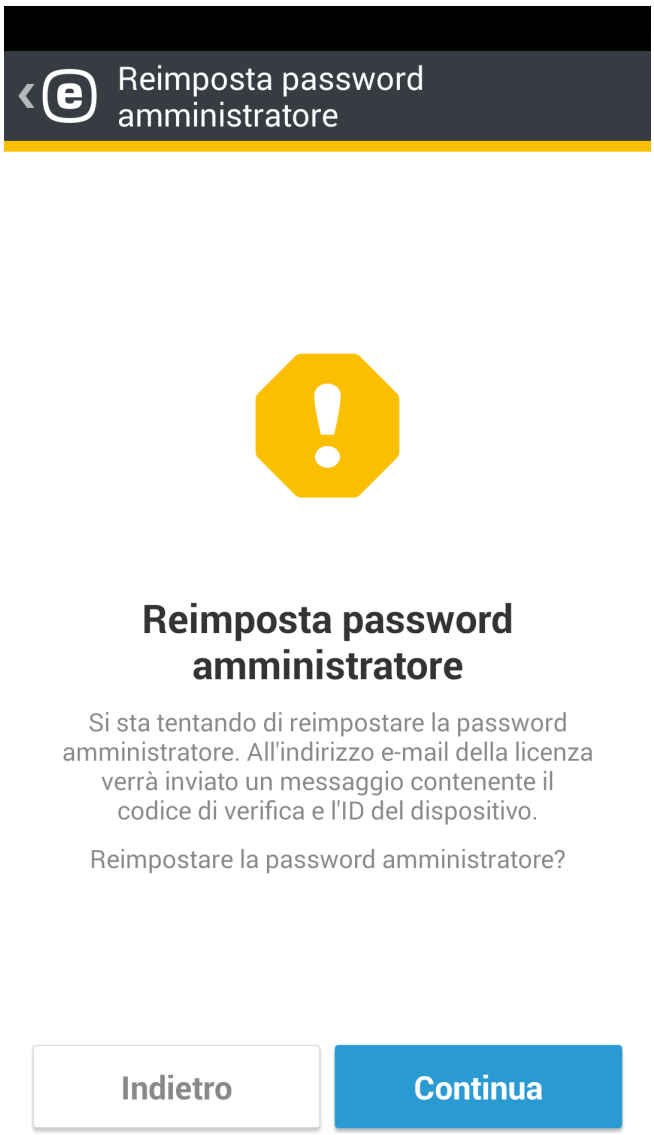
13.2 Password amministratore

La **Password amministratore** è necessaria per sbloccare un dispositivo, inviare comandi Anti-Furto, accedere a funzioni protette con password e disinstallare ESET Endpoint Security.

IMPORTANTE: scegliere la password con estrema attenzione. Per potenziare il livello di protezione e impedire a terzi di indovinarla facilmente, utilizzare una combinazione di lettere minuscole, lettere maiuscole e numeri.

Per reimpostare la password amministratore su un dispositivo con una schermata bloccata:

1. Toccare **Password dimenticata?** > **Continua** > **Richiedi codice di verifica**. Se il dispositivo non è connesso a Internet, toccare invece il collegamento **scegliere la reimpostazione off-line** e contattare il Supporto tecnico ESET.
2. Controllare la casella di posta: un'e-mail contenente il codice di verifica e l'ID del dispositivo verrà inviata all'indirizzo di posta elettronica associato alla licenza ESET. Il codice di verifica sarà attivo per 1 ora dal momento della ricezione.
3. Inserire il codice di verifica e una nuova password nella scherma bloccata del dispositivo.



13.3 Remote administrator

ESET Remote Administrator (ERA) consente all'utente di gestire ESET Endpoint Security in un ambiente di rete da una posizione centrale.

L'utilizzo di ERA non consente solo di potenziare il livello di protezione, ma offre anche una facilità di gestione di tutti i prodotti ESET installati sulle workstation client e sui dispositivi mobili. I dispositivi su cui è installato ESET Endpoint Security possono connettersi a ERA attraverso qualsiasi tipo di connessione Internet (WiFi, LAN, WLAN), rete cellulare (3G, 4G, HSDPA, GPRS), ecc., a condizione che la connessione sia regolare (senza proxy o firewall) e che entrambi gli endpoint siano configurati correttamente.

In caso di connessione a ERA su una rete cellulare, il livello di efficienza della connessione dipenderà dal provider della rete mobile e offrirà funzionalità complete.

Per connettere un dispositivo a ERA, aggiungerlo all'elenco **Computer** in ERA Web Console, registrarlo tramite l'attività **Registrazione dispositivo** e immettere l'indirizzo del server Mobile Device Connector (MDC):

- **Host del server**: specificare il nome DNS completo o l'indirizzo IP pubblico del server sul quale è in esecuzione Mobile Device Connector (MDC). Il nome host può essere utilizzato solo in caso di connessione attraverso una rete Wi-Fi interna.
- **Porta del server**: consente di specificare la porta del server utilizzata per la connessione a Mobile Device Connector.

NOTA: Ulteriori informazioni sulle modalità di gestione della rete attraverso l'utilizzo di ESET Remote Administrator, consultare la documentazione on-line di ESET Remote Administrator.

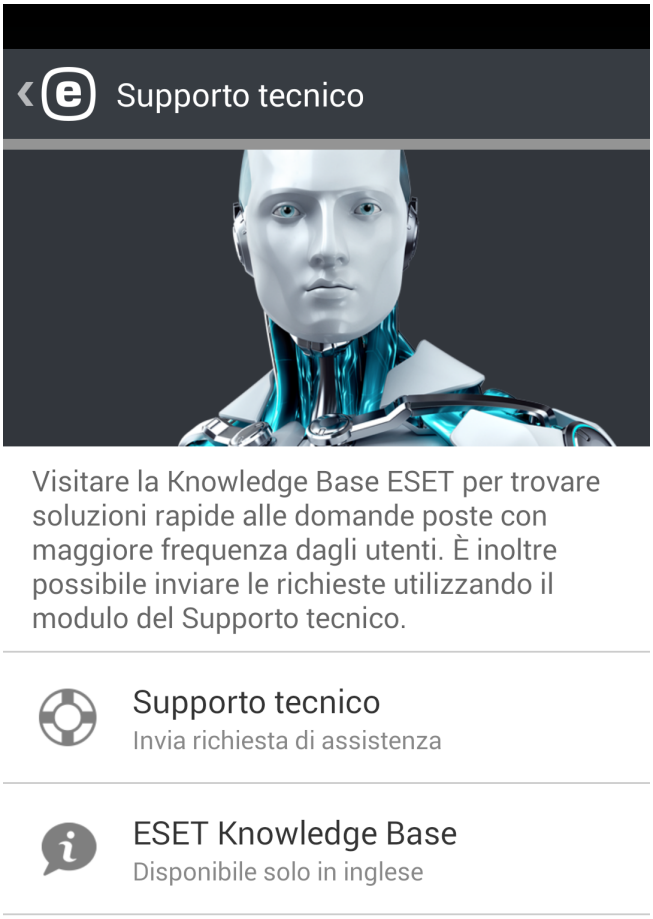
13.4 ID dispositivo

L'ID dispositivo consente all'amministratore di identificare il dispositivo dell'utente in caso di furto o smarrimento.

14. Supporto tecnico

Gli specialisti del Supporto tecnico ESET sono a disposizione degli utenti per fornire assistenza amministrativa o tecnica correlata a ESET Endpoint Security o a qualsiasi altro prodotto ESET.

Per inviare una richiesta di assistenza direttamente dal dispositivo in uso, toccare l'icona del menu nella schermata principale di ESET Endpoint Security (oppure premere il pulsante MENU sul dispositivo in uso), toccare **Supporto tecnico** > **Supporto tecnico** e compilare tutti i campi obbligatori.



ESET Endpoint Security include una funzionalità di registrazione avanzata che consente di diagnosticare problemi tecnici potenziali. Per fornire a ESET un rapporto dettagliato dell'applicazione, assicurarsi di aver selezionato **Invia rapporto applicazione** (impostazione predefinita). Toccare **Invia** per inviare la richiesta. Uno specialista del Supporto tecnico ESET contatterà l'utente all'indirizzo e-mail fornito.