kaspersky

Kaspersky Security for Mobile

Sommario

Guida di Kaspersky Security for Mobile

Kaspersky Security for Mobile è destinato alla protezione e alla gestione dei dispositivi mobili aziendali, nonché dei dispositivi mobili personali utilizzati dai dipendenti dell'azienda per scopi aziendali.

I componenti e le funzionalità di Kaspersky Security for Mobile dipendono dalla console di Kaspersky Security Center utilizzata come interfaccia per la protezione e la gestione dei dispositivi mobili.

Selezionare la sezione della Guida necessaria, a seconda della console di Kaspersky Security Center utilizzata:

- Administration Console basata su Microsoft Management Console
- Kaspersky Security Center Web Console o Kaspersky Security Center Cloud Console

Sezioni separate della Guida descrivono le funzionalità e le operazioni disponibili per gli utenti dell'app Kaspersky Endpoint Security for Android e dell'app Kaspersky Security for iOS.

Novità

Kaspersky Security for iOS Technical Release 1

La nuova app Kaspersky Security for iOS è destinata a proteggere e gestire i dispositivi iOS e iPadOS aziendali. L'app offre le seguenti funzionalità chiave:

- Protezione dalle minacce online.
- Rilevamento jailbreak.
- Gestione dei dispositivi aziendali con Kaspersky Security Center Web Console e Cloud Console.

Kaspersky Endpoint Security for Android Technical Release 42

- Miglioramenti dell'interfaccia utente nell'app Kaspersky Endpoint Security for Android.
- L'app Kaspersky Endpoint Security for Android adesso richiede l'autorizzazione "Dispositivi Bluetooth nelle vicinanze" in Android 12 o versione successiva per consentire all'amministratore di limitare l'utilizzo del Bluetooth.
- Correzioni di bug generali e miglioramenti.

Kaspersky Endpoint Security for Android Technical Release 41

- Miglioramenti dell'interfaccia utente nell'app Kaspersky Endpoint Security for Android.
- Miglioramenti dell'interfaccia utente nelle impostazioni dei criteri del plug-in di Kaspersky Security for Mobile (Policies) per Kaspersky Security Center Web Console e Cloud Console.
- Correzioni di bug generali e miglioramenti.

Kaspersky Endpoint Security for Android Technical Release 40

- Correzioni di bug generali e miglioramenti.

Kaspersky Endpoint Security for Android Technical Release 39

- Adesso è supportato Android 12L.
- Sono stati aggiornati i contratti e le informative seguenti:
  - Contratto di licenza con l'utente finale
  - Informativa di Kaspersky Security Network
  - Informativa relativa all'elaborazione dei dati per finalità di marketing

Tenere presente che l'amministratore può accettare i nuovi termini dei contratti e delle informative in Administration Console. In tal modo gli utenti dell'app Kaspersky Endpoint Security for Android potranno saltare questo passaggio nei dispositivi.

- Correzioni di bug generali e miglioramenti.

Kaspersky Endpoint Security for Android Technical Release 33

- Quando si gestisce l'app Kaspersky Endpoint Security for Android utilizzando sistemi EMM di terze parti, adesso è possibile accettare più Contratti di licenza con l'utente finale utilizzando un singolo comando.
- Non è più necessaria una chiave per attivare Samsung KNOX.
- La struttura delle versioni dei componenti di Kaspersky Security for Mobile è stata modificata per includere il numero di versione.

Kaspersky Endpoint Security for Android Technical Release 32

- L'app Kaspersky Endpoint Security for Android è stata modificata per supportare i requisiti Android aggiornati.

Kaspersky Endpoint Security for Android Technical Release 31

- Se Kaspersky Security Center non è distribuito nell'organizzazione o non è accessibile ai dispositivi mobili, gli utenti possono attivare manualmente l'app Kaspersky Endpoint Security for Android nei propri dispositivi.
- Kaspersky Security for Mobile adesso supporta la funzionalità Schede personalizzate di Google Chrome.

Kaspersky Endpoint Security for Android Technical Release 30

- Kaspersky Security for Mobile ora consente di proteggere e gestire i dispositivi mobili in Kaspersky Security Center Cloud Console.
- Kaspersky Security for Mobile adesso supporta iOS 15 e iPadOS 15.

Kaspersky Endpoint Security for Android Technical Release 29

- L'app Kaspersky Endpoint Security for Android adesso supporta Android 12.

Kaspersky Endpoint Security for Android Technical Release 27

- Kaspersky Security for Mobile ora consente di proteggere e gestire i dispositivi mobili in Kaspersky Security Center Web Console.

Kaspersky Endpoint Security for Android Technical Release 26

- Kaspersky Endpoint Security ora supporta licenze e abbonamenti con rinnovo automatico.

Kaspersky Endpoint Security for Android Technical Release 22

- Kaspersky Endpoint Security adesso supporta Kaspersky Private Security Network, una soluzione che consente l'accesso ai database di reputazione di Kaspersky Security Network senza l'invio dei dati al di fuori della rete aziendale.
- Kaspersky Endpoint Security for Android non supporta più l'installazione nei dispositivi che eseguono le versioni di Android 4.2 - 4.4.4.

Kaspersky Endpoint Security for Android Technical Release 20

- Agli utenti non viene richiesto di accettare informative legali se l'amministratore ha scelto di accettare le informative a livello globale.
- Le prestazioni dell'app sono state ottimizzate.

Kaspersky Endpoint Security for Android Technical Release 19

- L'amministratore adesso può accettare l'informativa di Kaspersky Security Network e altre informative per conto degli utenti finali tramite Kaspersky Security Center.
- Sono stati corretti diversi errori e la stabilità operativa è stata migliorata.

Kaspersky Endpoint Security for Android Technical Release 18

- Kaspersky Security for Mobile adesso supporta Huawei Mobile Services.
- Kaspersky Endpoint Security for Android adesso può essere installato da Huawei AppGallery.

Kaspersky Endpoint Security for Android Technical Release 17

- Kaspersky Endpoint Security adesso ha come destinazione l'API livello 29 e superiori, determinando alcune modifiche nel comportamento dell'app nei dispositivi che eseguono Android 10 o versioni successive.
- Nuove impostazioni di complessità della password per l'impostazione di password della complessità richiesta da parte dell'utente.
- La configurazione dell'utilizzo dell'impronta digitale come metodo di sblocco dello schermo è ora disponibile solo per il profilo lavoro Android.
- Sono stati corretti diversi errori e la stabilità operativa è stata migliorata.

Kaspersky Endpoint Security for Android Technical Release 16

- Kaspersky Endpoint Security for Android adesso supporta Android 11.
- Nuovi requisiti per le autorizzazioni relative a geolocalizzazione e fotocamera stabiliti da Android 11. Ulteriori informazioni sulle nuove regole per le autorizzazioni di accesso alla fotocamera e alla posizione sono disponibili in questa sezione.

- Adesso è possibile specificare gli indirizzi e-mail aziendali degli utenti in una console EMM di terze parti. Questi indirizzi e-mail verranno visualizzati in Kaspersky Security Center a condizione che il nuovo KscCorporateEmail sia configurato.

Kaspersky Endpoint Security for Android Technical Release 14

- Quando un utente consente o revoca i privilegi Amministratore dispositivo dell'app, viene inviato un evento alla Console di gestione.
- Il parametro "KscGroup" adesso può essere configurato in console EMM di terze parti. Quando un dispositivo si connette a Kaspersky Security Center, viene automaticamente aggiunto a una sottocartella della cartella Dispositivi non assegnati con lo stesso nome del gruppo configurato in una console EMM.

Kaspersky Endpoint Security for Android Technical Release 13

- Nuovo design dell'interfaccia utente per Kaspersky Endpoint Security for Android.
- Adesso tutte le sezioni della guida si trovano online.
- Gli indirizzi IP dei dispositivi gestiti adesso vengono inviati a Kaspersky Security Center e possono essere visualizzati nelle sezioni delle info sui dispositivi.

Kaspersky Endpoint Security for Android Technical Release 12

- È stata aggiunta la possibilità di accettare il Contratto di licenza con l'utente finale in Kaspersky Security Center 12.1 in remoto. Se l'amministratore accetta i termini del Contratto di licenza e dell'Informativa sulla privacy in Administration Console, l'app ignora questi passaggi durante il processo di installazione.
- È stata aggiunta la possibilità di modificare il nome del dispositivo in Kaspersky Security Center per gli utenti che utilizzano VMware AirWatch. È stata aggiunta una nuova impostazione al file di configurazione, utilizzato per configurare l'app. È possibile aggiungere altre informazioni al nome del dispositivo (ad esempio il numero di serie del dispositivo). In questo modo è più semplice individuare e ordinare i dispositivi in Kaspersky Security Center.

Kaspersky Endpoint Security for Android Technical Release 11

Sono stati corretti diversi errori e la stabilità operativa è stata migliorata.

Kaspersky Endpoint Security for Android Technical Release 10

- Kaspersky Security for Mobile ora supporta Kaspersky Security Center 12.
- Il supporto per Kaspersky Safe Browser è stato interrotto in Kaspersky Security Center 12. È possibile utilizzare le funzioni di Kaspersky Safe Browser quando si utilizza Kaspersky Security Center 11 o versioni precedenti.
- Sono stati corretti diversi errori e la stabilità operativa è stata migliorata.

Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3

- Supporto verificato di Kaspersky Endpoint Security for Android in Microsoft Intune (una soluzione (EMM) Enterprise Mobility Management). Kaspersky partecipa alla community AppConfig per garantire il funzionamento dell'app con soluzioni EMM di terze parti.

- È stata aggiunta la possibilità di disabilitare le notifiche e i messaggi pop-up quando l'app è in background. Tenere presente che non è prudente eseguire queste azioni in background. Se si disabilitano le notifiche e i messaggi pop-up quando l'app è in background, l'app non avviserà gli utenti delle minacce in tempo reale. Gli utenti dei dispositivi mobili possono scoprire lo stato della protezione del dispositivo solo quando aprono l'app.

- È stata aggiunta la possibilità di accettare il Contratto di licenza con l'utente finale e l'Informativa sulla privacy in VMware AirWatch. Se l'amministratore ha accettato il Contratto di licenza e l'Informativa sulla privacy nella console AirWatch, Kaspersky Endpoint Security for Android ignorerà il passaggio di accettazione nella Configurazione iniziale guidata.

- È stata aggiunta l'Informativa relativa all'elaborazione dei dati a scopo di utilizzo di Protezione Web (Informativa di Protezione Web). È necessario accettare l'informativa per utilizzare Protezione Web. Kaspersky Endpoint Security for Android utilizza Kaspersky Security Network (KSN) per eseguire la scansione dei siti Web. L'Informativa di Protezione Web contiene i termini e le condizioni dello scambio di dati con KSN. È possibile accettare l'Informativa di Protezione Web nel criterio o richiedere l'accettazione da parte dell'utente del dispositivo.

- Sono stati corretti diversi errori e la stabilità operativa è stata migliorata.

Confronto tra le funzionalità dell'applicazione in base agli strumenti di gestione

È possibile gestire i dispositivi mobili in Kaspersky Security Center utilizzando i seguenti strumenti di gestione:

- Administration Console di Kaspersky Security Center basata su Microsoft Management Console (di seguito denominata "basata su MMC")
- Kaspersky Security Center Web Console
- Kaspersky Security Center Cloud Console

La seguente tabella mette a confronto le funzionalità disponibili in questi strumenti.

Disponibilità delle funzionalità in base agli strumenti di gestione

	Console basata su MMC	Web Console	Cloud Console
Generale			
Gestione dispositivi Android	Disponibile	Disponibile	Disponibile
Gestione dispositivi iOS	Disponibile (tramite un certificato APNs)	Disponibile (tramite l'app Kaspersky Security for iOS)	Disponibile (tramite l'app Kaspersky Security for iOS)
Gestione dispositivi mobili			
Aggiunta di dispositivi utilizzando un collegamento a Google Play	Disponibile	Disponibile	Disponibile
Aggiunta di dispositivi tramite un collegamento all'App Store	Non disponibile	Disponibile	Disponibile
Aggiunta di dispositivi iOS tramite un profilo MDM iOS	Disponibile	Non disponibile	Non disponibile
Aggiunta di dispositivi tramite la creazione di un pacchetto di installazione	Disponibile	Non disponibile	Non disponibile
Invio di comandi ai dispositivi mobili	Disponibile	Disponibile (ad eccezione del comando Foto utente)	Disponibile (ad eccezione del comando Foto utente)
Rimozione dei dispositivi mobili da Kaspersky Security Center	Disponibile	Disponibile (Rimozione solo dall'elenco dei dispositivi. L'app deve essere rimossa manualmente dal dispositivo.)	Disponibile (Rimozione solo dall'elenco dei dispositivi. L'app deve essere rimossa manualmente dal dispositivo.)
Gestione dei certificati			
Emissione di certificati di posta	Disponibile	Non disponibile	Non disponibile
Emissione di certificati VPN	Disponibile	Non disponibile	Non disponibile

Emissione di certificati mobili	Disponibile	Disponibile	Disponibile
Emissione di certificati mobili tramite gli strumenti di Administration Server	Disponibile	Disponibile	Disponibile
Specificazione dei file di certificato	Disponibile	Non disponibile	Non disponibile
Integrazione con l'infrastruttura a chiave pubblica	Disponibile	Non disponibile	Non disponibile
Gestione dei criteri			
Accesso basato sui ruoli per la configurazione dei criteri di gruppo	Disponibile	Non disponibile	Non disponibile
Configurazione della sincronizzazione dei dispositivi mobili con Kaspersky Security Center	Disponibile	Disponibile	Disponibile
Configurazione delle scansioni virus nei dispositivi mobili	Disponibile	Disponibile	Disponibile
Configurazione della protezione dei dispositivi mobili	Disponibile	Disponibile	Disponibile
Configurazione degli aggiornamenti dei database anti-virus	Disponibile	Disponibile	Disponibile
Configurazione della protezione dei dati di un dispositivo rubato o smarrito	Disponibile	Disponibile	Disponibile
Configurazione dell'accesso dell'utente ai siti Web	Disponibile	Disponibile	Disponibile
Configurazione del controllo app	Disponibile	Disponibile	Disponibile
Configurazione del controllo conformità	Disponibile	Disponibile	Disponibile
Configurazione dei profili lavoro Android	Disponibile	Non disponibile	Non disponibile
Configurazione della connessione a una rete Wi-Fi	Disponibile	Non disponibile	Non disponibile
Samsung KNOX	Disponibile	Non disponibile	Non disponibile
Altre funzionalità			
Accettazione globale del Contratto di licenza con l'utente finale in Kaspersky Security Center	Disponibile	Non disponibile	Non disponibile
Configurazione di Kaspersky	Disponibile	Non disponibile	Non disponibile

Private Security Network			

Kit di distribuzione

Il kit di distribuzione di Kaspersky Security for Mobile può includere vari componenti, a seconda della versione dell'applicazione scelta.

Mobile Device Management in Kaspersky Security Center Web Console

- `on_prem_ksm_devices_xx.x.x.x.zip`

  Archivio che contiene i file necessari per l'installazione del plug-in di Kaspersky Security for Mobile (Devices):

  - `plugin.zip`

    Archivio che contiene il plug-in di Kaspersky Security for Mobile (Devices).

  - `signature.txt`

    File che contiene la firma per il plug-in di Kaspersky Security for Mobile (Devices).

- `on_prem_ksm_policies_xx.x.x.x.zip`

  Archivio che contiene i file necessari per l'installazione del plug-in di Kaspersky Security for Mobile (Policies):

  - `plugin.zip`

    Archivio che contiene il plug-in di Kaspersky Security for Mobile (Policies).

  - `signature.txt`

    File che contiene la firma per il plug-in di Kaspersky Security for Mobile (Policies).

Mobile Device Management in Kaspersky Security Center Cloud Console

Per gestire il dispositivo mobile in Kaspersky Security Center Cloud Console, non è necessario scaricare un pacchetto di distribuzione. È sufficiente creare un account in Kaspersky Security Center Cloud Console. Per ulteriori informazioni sulla creazione di un account, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

Mobile Device Management in Administration Console basata su MMC

- `Klcfginst_en.exe`

  Programma di installazione del plug-in di amministrazione di Kaspersky Endpoint Security for Android per gestire l'applicazione tramite il sistema di amministrazione remota Kaspersky Security Center.

- `Klmdminst.exe`

  Programma di installazione del plug-in di amministrazione di Kaspersky Device Management for iOS per gestire l'applicazione tramite il sistema di amministrazione remota Kaspersky Security Center.

File dell'app Kaspersky Endpoint Security for Android

`KES10_xx_xx_xxx.apk`: file del pacchetto Android dell'app Kaspersky Endpoint Security for Android.

File ausiliari

- `sc_package_xx.exe`

  Archivio autoestraente che contiene i file necessari per l'installazione dell'app Kaspersky Endpoint Security for Android creando i pacchetti di installazione:

  - `adb.exe, AdbWinApi.dll, AdbWinUsbApi.dll`

    File necessari per la creazione dei pacchetti di installazione.

  - `installer.ini`

    File di configurazione che contiene le impostazioni di connessione ad Administration Server.

  - `KES10_xx_xx_xxx.apk`

    File del pacchetto Android dell'app Kaspersky Endpoint Security for Android.

  - `kmlisten.exe`

    Utilità per la distribuzione dei pacchetti di installazione tramite il computer dell'amministratore.

  - `kmlisten.ini`

    File di configurazione che contiene le impostazioni per l'utilità `kmlisten.exe`.

  - `kmlisten.kpd`

    File di descrizione dell'applicazione.

- `SigningUtility.zip`

  Archivio che contiene l'utilità per firmare i pacchetti di distribuzione dell'app Kaspersky Endpoint Security for Android e i contenitori per i dispositivi iOS.

Documentazione

- Guida per Kaspersky Security for Mobile.

Utilizzo di Kaspersky Security Center Web Console e Kaspersky Security Center Cloud Console

Questa sezione della Guida descrive la protezione e la gestione dei dispositivi mobili offerte da Kaspersky Security Center Web Console (di seguito denominato anche Web Console) o Kaspersky Security Center Cloud Console (di seguito denominato anche Cloud Console).

Informazioni su Mobile Device Management in Kaspersky Security Center Web Console e Cloud Console

È possibile gestire i dispositivi mobili in Kaspersky Security Center Web Console e Cloud Console utilizzando i seguenti componenti:

- **App Kaspersky Endpoint Security for Android**

  L'app Kaspersky Endpoint Security for Android garantisce la protezione dei dispositivi mobili da minacce Web, virus e altri programmi che rappresentano minacce.

- **App Kaspersky Security for iOS**

  L'app Kaspersky Security for iOS garantisce la protezione dei dispositivi mobili da phishing e malware.

- **Plug-in di Kaspersky Security for Mobile (Devices)**

  Il plug-in di Kaspersky Security for Mobile (Devices) fornisce l'interfaccia per la gestione dei dispositivi mobili e delle app mobili installate tramite Kaspersky Security Center Web Console e Cloud Console.

- **Plug-in di Kaspersky Security for Mobile (Policies)**

  Il plug-in di Kaspersky Security for Mobile (Policies) consente di definire le impostazioni di configurazione per i dispositivi connessi a Kaspersky Security Center utilizzando criteri di gruppo.

I plug-in sono integrati nel *sistema di amministrazione remota Kaspersky Security Center*. È possibile utilizzare Kaspersky Security Center Web Console o Cloud Console per gestire dispositivi mobili, nonché computer client e sistemi virtuali. In seguito alla connessione all'Administration Server, i dispositivi mobili diventano gestiti. È possibile monitorare in remoto i dispositivi gestiti.

Funzionalità chiave per la gestione dei dispositivi mobili in Kaspersky Security Center Web Console e Cloud Console

Kaspersky Security for Mobile offre le seguenti funzionalità:

- Distribuzione di messaggi e-mail per la connessione dei dispositivi mobili Android a Kaspersky Security Center utilizzando i collegamenti per scaricare l'app Kaspersky Endpoint Security for Android da Google Play.
- Distribuzione di messaggi e-mail per la connessione dei dispositivi mobili iOS a Kaspersky Security Center utilizzando i collegamenti per scaricare l'app Kaspersky Security for iOS dall'App Store.
- Connessione remota dei dispositivi mobili a Kaspersky Security Center e altri sistemi EMM di terze parti (ad esempio VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).
- Configurazione remota dell'app mobile e configurazione remota di servizi, app e funzioni dei dispositivi mobili.

- Configurazione remota dei dispositivi mobili in base ai requisiti di sicurezza aziendale.
- Impedimento della fuga di informazioni aziendali memorizzate nei dispositivi mobili, in caso di furto o smarrimento (Antifurto). Supporto previsto solo per i dispositivi Android.
- Controllo della conformità ai requisiti di sicurezza aziendali (Controllo conformità). Supporto previsto solo per i dispositivi Android.
- Controllo della protezione contro le minacce online e controllo dell'utilizzo di Internet nei dispositivi mobili (Protezione Web).
- Configurazione delle notifiche mostrate all'utente nelle app Kaspersky Endpoint Security for Android e Kaspersky Security for iOS.
- Le notifiche dell'amministratore sullo stato e gli eventi delle app Kaspersky Endpoint Security for Android e Kaspersky Security for iOS possono essere comunicate in Kaspersky Security Center o tramite e-mail.
- Controllo delle modifiche per le impostazioni dei criteri (cronologia delle revisioni).

Kaspersky Security for Mobile include i seguenti componenti di gestione e protezione:

- Anti-Virus (per dispositivi Android)
- Antifurto (per dispositivi Android)
- Protezione Web (per dispositivi Android e iOS)
- Controllo app (per dispositivi Android)
- Controllo conformità (per dispositivi Android)
- Rilevamento dei privilegi di root nei dispositivi Android e rilevamento di jailbreak nei dispositivi iOS

Informazioni sull'app Kaspersky Endpoint Security for Android

L'app Kaspersky Endpoint Security for Android garantisce la protezione dei dispositivi mobili da minacce Web, virus e altri programmi che rappresentano minacce.

L'app Kaspersky Endpoint Security for Android include i seguenti componenti:

- **Anti-Virus**. Questo componente consente di rilevare e neutralizzare le minacce nel dispositivo utilizzando i database anti-virus e il servizio cloud Kaspersky Security Network. Anti-Virus include i seguenti componenti:
  - **Protezione**. Rileva le minacce nei file aperti, esamina le nuove app e protegge in tempo reale i dispositivi dalle infezioni.
  - **Scansione**. Viene avviata su richiesta per l'intero file system, solo per le app installate o per un file o una cartella in particolare.
  - **Aggiornamento**. Consente all'utente di scaricare nuovi database anti-virus per l'applicazione.
- **Antifurto**. Questo componente protegge le informazioni sul dispositivo dall'accesso non autorizzato in caso di furto o smarrimento del dispositivo. Questo componente consente di inviare i seguenti comandi al dispositivo:

- **Localizza**. Consente di ottenere le coordinate della posizione del dispositivo.
- **Allarme**. Fa in modo che il dispositivo emetta un forte allarme.
- **Cancella**. Consente di cancellare i dati aziendali per proteggere le informazioni aziendali sensibili.

- **Protezione Web**. Questo componente blocca i siti Web dannosi progettati per diffondere codice dannoso. Protezione Web blocca anche i siti Web contraffatti (di phishing) progettati per rubare informazioni riservate (ad esempio, password di online banking o sistemi e-money) e ottenere l'accesso alle informazioni finanziarie dell'utente. Protezione Web analizza i siti Web prima dell'apertura utilizzando il servizio cloud Kaspersky Security Network. Dopo la scansione, Protezione Web consente il caricamento dei siti Web ritenuti attendibili e blocca i siti Web dannosi. Protezione Web supporta inoltre il filtro dei siti Web in base alle categorie definite nel servizio cloud Kaspersky Security Network. Questo consente all'amministratore di limitare l'accesso dell'utente a determinate categorie di pagine Web (ad esempio, alle pagine Web delle categorie "Gioco d'azzardo, lotterie, scommesse" o "Comunicazioni di rete").
- **Controllo app.** Questo componente consente di installare le app consigliate e richieste nel dispositivo tramite un collegamento diretto al pacchetto di distribuzione o tramite un collegamento a Google Play. Controllo app consente di rimuovere le app bloccate che violano i requisiti di sicurezza aziendali.
- **Controllo conformità.** Questo componente consente di verificare la conformità dei dispositivi gestiti con i requisiti di sicurezza aziendali e di imporre restrizioni su determinate funzioni dei dispositivi non conformi.

È possibile configurare i componenti dell'app Kaspersky Endpoint Security for Android in Kaspersky Security Center Web Console e Cloud Console definendo le impostazioni dei criteri di gruppo.

Informazioni sull'app Kaspersky Security for iOS

L'app Kaspersky Security for iOS garantisce la protezione dei dispositivi mobili da phishing e malware.

L'app Kaspersky Security for iOS offre le seguenti funzionalità chiave:

- **Protezione Web**. Questo componente blocca i siti Web dannosi progettati per diffondere codice dannoso. Protezione Web blocca anche i siti Web contraffatti (di phishing) progettati per rubare informazioni riservate (ad esempio, password di online banking o sistemi e-money) e ottenere l'accesso alle informazioni finanziarie dell'utente. Protezione Web analizza i siti Web prima dell'apertura utilizzando il servizio cloud Kaspersky Security Network. Dopo la scansione, Protezione Web consente il caricamento dei siti Web ritenuti attendibili e blocca i siti Web dannosi. È possibile configurare questo componente in Kaspersky Security Center Web Console definendo le impostazioni dei criteri di gruppo.
- **Rilevamento jailbreak**. Quando Kaspersky Security for iOS rileva un jailbreak, visualizza un messaggio critico e informa l'utente del problema.

Informazioni sul plug-in di Kaspersky Security for Mobile (Devices)

Il plug-in di Kaspersky Security for Mobile (Devices) fornisce l'interfaccia per la gestione dei dispositivi mobili e delle app mobili installate tramite Kaspersky Security Center Web Console e Cloud Console. Il plug-in di Kaspersky Security for Mobile (Devices) consente di eseguire le seguenti operazioni:

- Connettere i dispositivi mobili a Kaspersky Security Center.
- Gestire i certificati dei dispositivi mobili.

- Configurare Firebase Cloud Messaging (solo per i dispositivi Android).
- Inviare comandi ai dispositivi mobili (solo per i dispositivi Android).

Il plug-in di Kaspersky Security for Mobile (Devices) può essere installato durante la configurazione di Kaspersky Security Center Web Console. Se si utilizza Kaspersky Security Center Cloud Console, non è necessario installare questo plug-in. Per ulteriori informazioni sugli scenari di distribuzione nei diversi tipi di console, vedere la sezione "Scenari di distribuzione".

Informazioni sul plug-in di Kaspersky Security for Mobile (Policies)

Il plug-in di Kaspersky Security for Mobile (Policies) consente di definire le impostazioni di configurazione per i dispositivi connessi a Kaspersky Security Center utilizzando criteri di gruppo. Il plug-in di Kaspersky Security for Mobile (Policies) può essere utilizzato per eseguire le seguenti operazioni:

- Creare criteri di sicurezza di gruppo per i dispositivi mobili.
- Configurare in remoto le impostazioni operative dell'app mobile nei dispositivi mobili degli utenti.
- Ricevere rapporti e statistiche sul funzionamento dell'app mobile nei dispositivi mobili degli utenti.

Il plug-in di Kaspersky Security for Mobile (Policies) può essere installato durante la configurazione di Kaspersky Security Center Web Console. Se si utilizza Kaspersky Security Center Cloud Console, non è necessario installare questo plug-in. Per ulteriori informazioni sugli scenari di distribuzione nei diversi tipi di console, vedere la sezione "Scenari di distribuzione".

Requisiti hardware e software

Questa sezione elenca i requisiti hardware e software per il computer dell'amministratore utilizzato per installare il plug-in di Kaspersky Security for Mobile (Devices) e il plug-in di Kaspersky Security for Mobile (Policies) in Kaspersky Security Center Web Console e Cloud Console, nonché i requisiti hardware e software delle app mobili.

Requisiti hardware e software per il computer dell'amministratore

Per installare il plug-in di Kaspersky Security for Mobile (Devices) e il plug-in di Kaspersky Security for Mobile (Policies), il computer dell'amministratore deve soddisfare i requisiti hardware di Kaspersky Security Center. Per ulteriori informazioni sui requisiti hardware e software di Kaspersky Security Center:

- Se si utilizza Kaspersky Security Center Web Console, fare riferimento alla *Guida di Kaspersky Security Center*.
- Se si utilizza Kaspersky Security Center Cloud Console, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

Per utilizzare il plug-in di Kaspersky Security for Mobile (Devices) e il plug-in di Kaspersky Security for Mobile (Policies) in Kaspersky Security Center Web Console, è necessario installare Kaspersky Security Center Web Console nel computer dell'amministratore.

Per utilizzare il plug-in di Kaspersky Security for Mobile (Devices) e il plug-in di Kaspersky Security for Mobile (Policies) in Kaspersky Security Center Cloud Console, è necessario creare un account in Kaspersky Security Center Cloud Console. Per ulteriori informazioni sulla creazione di un account, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

L'app Kaspersky Endpoint Security for Android può funzionare nell'ambito dei seguenti sistemi EMM di terze parti:

- VMWare AirWatch 9.3 o versione successiva
- MobileIron 10.0 o successiva
- IBM MaaS360 10.68 o versione successiva
- Microsoft Intune 1908 o versione successiva
- SOTI MobiControl 14.1.4 (1693) o successiva

Requisiti hardware e software per consentire al dispositivo mobile dell'utente di supportare l'installazione dell'app Kaspersky Endpoint Security for Android

L'app Kaspersky Endpoint Security for Android presenta i seguenti requisiti hardware e software:

- Smartphone o tablet con una risoluzione dello schermo di 320x480 pixel o superiore
- 65 MB di spazio disponibile sul disco nella memoria principale del dispositivo
- Android 5.0–12 (compreso Android 12L, a esclusione di Go Edition)
- Architettura del processore x86, x86-64, Arm5, Arm6, Arm7 o Arm8

L'app può essere installata soltanto nella memoria principale del dispositivo.

Requisiti hardware e software per consentire al dispositivo mobile dell'utente di supportare l'installazione dell'app Kaspersky Security for iOS

L'app Kaspersky Security for iOS dispone dei seguenti requisiti hardware:

- iPhone 6S o versione successiva
- iPad Air 2 o versione successiva

L'app Kaspersky Security for iOS dispone dei seguenti requisiti software:

- iOS 14.1 o versione successiva
- iPadOS 14.1 o versione successiva

L'app Kaspersky Security for iOS non può funzionare correttamente quando un client VPN con una connessione VPN attiva è in esecuzione nello stesso dispositivo mobile.

Problemi noti e considerazioni

Kaspersky Endpoint Security for Android e Kaspersky Security for iOS presentano diversi problemi noti che non sono critici per il funzionamento di queste app.

Problemi noti di Kaspersky Security for iOS

- L'app Kaspersky Security for iOS non può funzionare correttamente quando un client VPN con una connessione VPN attiva è in esecuzione nello stesso dispositivo mobile.

Problemi noti di Kaspersky Endpoint Security for Android

Problemi noti all'avvio di Mobile Device Management in Kaspersky Security Center Web Console

- È possibile avviare Mobile Device Management durante la configurazione iniziale di Administration Console basata su MMC di Kaspersky Security Center (durante l'esecuzione dell'Avvio rapido guidato) o successivamente visualizzando la cartella Mobile Device Management in Administration Console.

Problemi noti durante l'installazione delle app

- Kaspersky Endpoint Security for Android viene installato solo nella memoria principale del dispositivo.
- Nei dispositivi che eseguono Android 7.0 potrebbe verificarsi un errore durante i tentativi di disabilitare i diritti di amministratore per Kaspersky Endpoint Security for Android nelle impostazioni del dispositivo se per Kaspersky Endpoint Security for Android è vietata la sovrapposizione con altre finestre. Questo problema è causato da un difetto ben noto in Android 7.
- Kaspersky Endpoint Security for Android nei dispositivi che eseguono Android 7.0 o versioni successive non supporta la modalità multi-finestra.
- Kaspersky Endpoint Security for Android non funziona nei dispositivi Chrome che eseguono il sistema operativo Chrome.
- Kaspersky Endpoint Security for Android non funziona nei dispositivi che eseguono il sistema operativo Android (Go Edition).
- Durante l'utilizzo dell'app Kaspersky Endpoint Security for Android con sistemi EMM di terze parti (ad esempio VMWare AirWatch), sono disponibili solo i componenti Anti-Virus e Protezione Web. L'amministratore può configurare le impostazioni di Anti-Virus e Protezione Web nella console di sistema EMM. In questo caso, le notifiche sul funzionamento dell'app sono disponibili solo nell'interfaccia dell'app Kaspersky Endpoint Security for Android (Rapporti).

Problemi noti durante l'upgrade della versione dell'app

- È possibile eseguire l'upgrade di Kaspersky Endpoint Security for Android solo a una versione più recente dell'app. Non è possibile eseguire il downgrade di Kaspersky Endpoint Security for Android a una versione precedente.

Problemi noti durante l'esecuzione di Anti-Virus

- A causa di limitazioni tecniche, Kaspersky Endpoint Security for Android non può esaminare file con dimensioni pari o superiori a 2 GB. Durante una scansione, l'app ignora tali file senza inviare una notifica in merito.

- Per un'ulteriore analisi di un dispositivo per il rilevamento delle nuove minacce per cui non sono ancora state aggiunte informazioni ai database anti-virus, è necessario abilitare l'utilizzo di Kaspersky Security Network. *Kaspersky Security Network (KSN)* è un'infrastruttura di servizi cloud che consente l'accesso alla Knowledge Base online di Kaspersky con informazioni sulla reputazione di file, risorse Web e software. Per l'utilizzo di KSN, il dispositivo mobile deve essere connesso a Internet.

- In alcuni casi, l'aggiornamento dei database anti-virus da Administration Server in un dispositivo mobile potrebbe non andare a buon fine. In questo caso, eseguire l'attività di aggiornamento dei database anti-virus in Administration Server.

- In alcuni dispositivi Kaspersky Endpoint Security for Android non rileva dispositivi connessi tramite USB OTG. Non è possibile eseguire una scansione virus in tali dispositivi.

- Nei dispositivi che eseguono Android 11.0 o versioni successive l'utente deve concedere l'autorizzazione "Consentire l'accesso per gestire tutti i file".

- Nei dispositivi che eseguono Android 7.0 o versioni successive la finestra di configurazione per la pianificazione dell'esecuzione delle scansioni virus potrebbe essere visualizzata in modo errato (gli elementi di gestione non sono visualizzati). Questo problema è causato da un difetto ben noto in Android 7.

- Nei dispositivi con Android 7.0, la protezione in tempo reale in modalità estesa non rileva le minacce presenti nei file archiviati in una scheda SD esterna.

- Nei dispositivi che eseguono Android 6.0 Kaspersky Endpoint Security for Android non rileva il download di un file dannoso nella memoria del dispositivo. Un file dannoso può essere rilevato da Anti-Virus al momento dell'esecuzione del file o nel corso di una scansione virus del dispositivo. Questo problema è causato da un difetto ben noto in Android 6.0. Per garantire la sicurezza del dispositivo, è consigliabile configurare scansioni virus pianificate.

Problemi noti durante l'esecuzione di Protezione Web

- Protezione Web nei dispositivi Android funziona solo nel browser Google Chrome (inclusa la funzionalità Schede personalizzate), in Huawei Browser e Samsung Internet Browser.

- Per il funzionamento di Protezione Web, è necessario abilitare l'utilizzo di Kaspersky Security Network. Protezione Web blocca i siti Web in base ai dati di KSN sulla reputazione e la categoria dei siti Web.

- I siti Web non consentiti potrebbero non essere bloccati da Protezione Web nei dispositivi che eseguono Android 6.0 con Google Chrome 51 (o versioni precedenti) se il sito Web viene aperto nei seguenti modi (questo problema è causato da un problema noto di Google Chrome):

  - Dai risultati di ricerca
  - Dall'elenco dei segnalibri
  - Dalla cronologia delle ricerche
  - Utilizzando la funzione di completamento automatico degli indirizzi Web
  - Aprendo il sito Web in una nuova scheda in Google Chrome

- I siti Web non consentiti potrebbero non essere bloccati in Google Chrome 50 (o versioni precedenti) se il sito Web viene aperto dalla pagina dei risultati di ricerca di Google mentre la funzionalità **Unisci schede e app** è abilitata nelle impostazioni del browser. Questo problema è causato da un difetto ben noto in Google Chrome.

- I siti Web delle categorie bloccate possono rimanere sbloccati in Google Chrome se l'utente li apre da app di terze parti, ad esempio da un'app del client IM. Questo problema è correlato alla modalità di esecuzione del servizio di accessibilità con la funzionalità Schede personalizzate di Chrome.

- I siti Web vietati possono rimanere sbloccati in Samsung Internet Browser se l'utente li apre in background dal menu di scelta rapida o da app di terze parti, ad esempio da un'app del client IM.

- Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità al fine di garantire il corretto funzionamento di Protezione Web.

- I siti Web consentiti possono essere bloccati nel browser Samsung Internet nella modalità di Protezione Web **Solo i siti Web elencati sono consentiti** quando la pagina viene aggiornata. I siti Web vengono bloccati se un'espressione regolare contiene impostazioni avanzate (ad esempio `^https?:\/\/example\.com\/pictures\/`). È consigliabile utilizzare espressioni regolari senza impostazioni aggiuntive (ad esempio `^https?:\/\/example\.com`).

Problemi noti durante l'esecuzione di Antifurto

- Per l'invio tempestivo dei comandi ai dispositivi Android, l'app utilizza il servizio Firebase Cloud Messaging (FCM). Se FCM non è configurato, i comandi verranno inviati al dispositivo solo durante la sincronizzazione con Kaspersky Security Center in base alla pianificazione definita nel criterio, ad esempio, ogni 24 ore).

- Per bloccare un dispositivo, Kaspersky Endpoint Security for Android deve essere impostato come amministratore del dispositivo.

- Per bloccare i dispositivi che eseguono Android 7.0 o versioni successive, Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità.

- In alcuni dispositivi l'esecuzione dei comandi di Antifurto può non andare a buon fine se nel dispositivo è abilitata la modalità Risparmio batteria. Questo difetto è stato confermato in Alcatel 5080X.

- Per localizzare i dispositivi che eseguono Android 10.0 o versioni successive, l'utente deve concedere l'autorizzazione "Sempre" per la localizzazione del dispositivo.

Problemi noti durante l'esecuzione di Controllo app

- Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità al fine di garantire il corretto funzionamento di Controllo app.

- Per il funzionamento di Controllo app (categorie di app), è necessario abilitare l'utilizzo di Kaspersky Security Network. Controllo app determina la categoria di un'app in base ai dati disponibili in KSN. Per l'utilizzo di KSN, il dispositivo mobile deve essere connesso a Internet. Per Controllo app, è possibile aggiungere singole app agli elenchi delle app bloccate e consentite. In questo caso, KSN non è necessario.

- Durante la configurazione di Controllo app, è consigliabile deselezionare la casella **Blocca app di sistema**. Il blocco delle app di sistema potrebbe generare problemi di funzionamento del dispositivo.

Problemi noti durante la configurazione della complessità della password di sblocco del dispositivo

- Nei dispositivi che eseguono Android 10.0 o versioni successive Kaspersky Endpoint Security risolve i requisiti di complessità della password in uno dei valori di sistema: medio o alto.

Se la lunghezza della password richiesta è compresa tra 1 e 4 simboli, l'app richiede all'utente di impostare una password di complessità media. Deve essere una password numerica (PIN) senza sequenze ripetute o ordinate (ad es. 1234) oppure alfanumerica. Il PIN o la password deve contenere almeno 4 caratteri.

Se la lunghezza della password richiesta è superiore a 5 simboli, l'app richiede all'utente di impostare una password di complessità alta. Deve essere una password numerica (PIN) senza sequenze ripetute o ordinate oppure alfanumerica (password). Il PIN deve contenere almeno 8 cifre; la password deve contenere almeno 6 caratteri.

- Nei dispositivi che eseguono Android 7.1.1 se la password di sblocco non soddisfa i requisiti di sicurezza aziendali (Controllo conformità), l'app di sistema Impostazioni può funzionare in modo errato quando si tenta di modificare la password di sblocco tramite Kaspersky Endpoint Security for Android. Il problema è causato da un difetto ben noto in Android 7.1.1. In questo caso, per modificare la password di sblocco, utilizzare solo l'app di sistema Impostazioni.

- In alcuni dispositivi che eseguono Android 6.0 o versioni successive può verificarsi un errore quando si immette la password di sblocco dello schermo se i dati del dispositivo sono criptati. Questo problema è correlato alle specifiche funzionalità del servizio di accessibilità con il firmware MIUI.

Problemi noti con la protezione dalla rimozione delle app

- Kaspersky Endpoint Security for Android deve essere impostato come amministratore del dispositivo.

- Per proteggere l'app dalla rimozione nei dispositivi che eseguono Android 7.0 o versioni successive, Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità.

- In alcuni dispositivi Xiaomi e Huawei, la protezione dalla rimozione di Kaspersky Endpoint Security for Android non funziona. Questo problema è causato da funzionalità specifiche del firmware MIUI 7 e 8 in Xiaomi e del firmware EMUI in Huawei.

Problemi noti durante la configurazione delle restrizioni relative ai dispositivi

- Nei dispositivi con Android 10.0 o versioni successive, il divieto di utilizzo delle reti Wi-Fi non è supportato.

- Nei dispositivi che eseguono Android 10.0 o versioni successive, l'utilizzo della fotocamera non può essere completamente vietato.

- Nei dispositivi che eseguono Android 11 o versioni successive Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo. In tal caso, non sarà possibile limitare l'utilizzo della fotocamera.

Problemi noti durante l'invio dei comandi ai dispositivi mobili

- Nei dispositivi che eseguono Android 12 o versioni successive, se l'utente ha concesso l'autorizzazione per l'utilizzo della posizione approssimativa, l'app Kaspersky Endpoint Security for Android cerca prima di ottenere la posizione esatta del dispositivo. Se l'operazione non va a buon fine, viene restituita la posizione approssimativa del dispositivo solo se è stata ricevuta non più di 30 minuti prima. In caso contrario, il comando di **Localizza dispositivo** non va a buon fine.

Problemi noti con dispositivi specifici

- In determinati dispositivi (ad esempio Huawei, Meizu e Xiaomi), è necessario concedere a Kaspersky Endpoint Security for Android un'autorizzazione di avvio automatico o aggiungere manualmente l'app all'elenco delle app eseguite all'avvio del sistema operativo. Se l'app non viene aggiunta all'elenco, Kaspersky Endpoint Security for Android interrompe l'esecuzione di tutte le funzioni in seguito al riavvio del dispositivo mobile. Inoltre, se il dispositivo è stato bloccato, non è possibile utilizzare un comando per sbloccarlo. È possibile sbloccare il dispositivo solo utilizzando un codice di sblocco monouso.

- In alcuni dispositivi (ad esempio, Meizu e Asus) con sistema operativo Android 6.0 o versione successiva, dopo il criptaggio dei dati e il riavvio del dispositivo Android, è necessario immettere una password numerica per sbloccare il dispositivo. Se l'utente utilizza una password grafica per sbloccare il dispositivo, è necessario convertire le password grafica in una password numerica. Per maggiori informazioni sulla conversione di una password grafica in una password numerica, fare riferimento al sito Web dell'assistenza tecnica del produttore del dispositivo mobile. Questo problema è correlato all'esecuzione del servizio per le funzionalità di accessibilità.

- In alcuni dispositivi Huawei che eseguono Android 5.X, dopo l'impostazione di Kaspersky Endpoint Security for Android come funzionalità di accessibilità potrebbe essere visualizzato un messaggio errato relativo alla mancanza dei diritti appropriati. Per nascondere questo messaggio, abilitare l'app come app protetta nelle impostazioni del dispositivo.

- In alcuni dispositivi Huawei con sistema operativo Android 5.X o 6.X, quando è abilitata la modalità Risparmio batteria per Kaspersky Endpoint Security for Android, l'utente può terminare manualmente l'app. In seguito a questa operazione, il dispositivo dell'utente diventa non protetto. Questo problema è dovuto ad alcune funzionalità del software Huawei. Per ripristinare la protezione del dispositivo, eseguire Kaspersky Endpoint Security for Android manualmente. È consigliabile disabilitare la modalità Risparmio batteria per Kaspersky Endpoint Security for Android nelle impostazioni del dispositivo.

- Nei dispositivi Huawei con firmware EMUI che eseguono Android 7.0 l'utente può nascondere la notifica relativa allo stato di protezione di Kaspersky Endpoint Security for Android. Questo problema è dovuto ad alcune funzionalità del software Huawei.

- In alcuni dispositivi Xiaomi, impostando una lunghezza della password superiore a 5 caratteri in un criterio, all'utente verrà richiesto di modificare la password di sblocco dello schermo invece del codice PIN. Non è possibile impostare un codice PIN con più di 5 caratteri. Questo problema è dovuto ad alcune funzionalità del software Xiaomi.

- Nei dispositivi Xiaomi con firmware MIUI che eseguono Android 6.0 l'icona di Kaspersky Endpoint Security for Android può essere nascosta nella barra di stato. Questo problema è dovuto ad alcune funzionalità del software Xiaomi. È consigliabile consentire la visualizzazione delle icone di notifica nelle impostazioni delle notifiche.

- In alcuni dispositivi Nexus che eseguono Android 6.0.1, i privilegi richiesti per il corretto funzionamento non possono essere concessi attraverso l'Avvio rapido guidato di Kaspersky Endpoint Security for Android. Il problema è causato da un difetto ben noto della patch di protezione per Android di Google. Per garantire il corretto funzionamento, è necessario concedere manualmente i privilegi richiesti nelle impostazioni del dispositivo.

- In alcuni dispositivi Samsung con Android 7.0 o versioni successive, quando l'utente tenta di configurare metodi non supportati per lo sblocco del dispositivo (ad esempio, una password grafica), il dispositivo può essere bloccato se vengono soddisfatte le seguenti condizioni: la protezione dalla rimozione di Kaspersky Endpoint Security for Android è abilitata e sono impostati requisiti per la complessità della password di sblocco dello schermo. Per sbloccare il dispositivo, è necessario inviare un comando speciale al dispositivo.

- In determinati dispositivi Samsung, non è possibile impedire l'utilizzo delle impronte digitali per lo sblocco dello schermo.

- Protezione Web non può essere abilitato in alcuni dispositivi Samsung se il dispositivo è connesso a una rete 3G/4G, se è abilitata la modalità Risparmio batteria e vengono limitati i dati in background. È consigliabile disabilitare la funzione che limita i processi in background nelle impostazioni di Risparmio batteria.

- In determinati dispositivi Samsung, se la password di sblocco non è conforme ai requisiti di sicurezza aziendali, Kaspersky Endpoint Security for Android non impedisce l'utilizzo delle impronte digitali per lo sblocco dello schermo.

- In alcuni dispositivi Honor e Huawei, non è possibile limitare l'utilizzo del Bluetooth. Quando Kaspersky Endpoint Security for Android tenta di limitare l'uso del Bluetooth, il sistema operativo visualizza una notifica contenente le opzioni per rifiutare o consentire la limitazione. L'utente può rifiutare questa limitazione e continuare a utilizzare il Bluetooth.

- Nei dispositivi Blackview l'utente può cancellare la memoria per l'app Kaspersky Endpoint Security for Android. Di conseguenza, la protezione e la gestione del dispositivo vengono disabilitate, tutte le impostazioni definite perdono validità e l'app Kaspersky Endpoint Security for Android viene rimossa dalle funzionalità di accessibilità. Questo avviene perché i dispositivi di questo fornitore contengono l'app Recent screens personalizzata con privilegi elevati. Questa app può sovrascrivere le impostazioni di Kaspersky Endpoint Security for Android e non può essere sostituita perché fa parte del sistema operativo Android.

- In alcuni dispositivi con Android 11, l'app Kaspersky Endpoint Security for Android si arresta in modo anomalo subito dopo l'avvio. Questo problema è causato da un difetto ben noto in Android 11.

Distribuzione di una soluzione Mobile Device Management in Kaspersky Security Center Web Console o Cloud Console

Per gestire i dispositivi mobili utilizzando Kaspersky Security Center Web Console o Cloud Console, è necessario distribuire una soluzione Mobile Device Management.

Scenari di distribuzione

Distribuzione in Kaspersky Security Center Web Console

La distribuzione della soluzione Mobile Device Management in Kaspersky Security Center Web Console prevede i seguenti passaggi:

1. Preparazione di Kaspersky Security Center Web Console per la distribuzione
2. Distribuzione dei plug-in di amministrazione
3. Distribuzione dell'app mobile
4. (Facoltativo, solo per Android) Configurazione dello scambio di informazioni con Firebase Cloud Messaging

   È consigliabile eseguire questo passaggio per garantire l'invio tempestivo dei comandi ai dispositivi mobili e la sincronizzazione forzata quando vengono modificate le impostazioni dei criteri.

Distribuzione in Kaspersky Security Center Cloud Console

La distribuzione della soluzione Mobile Device Management in Kaspersky Security Center Cloud Console prevede i seguenti passaggi:

1. Preparazione di Kaspersky Security Center Cloud Console per la distribuzione
2. Distribuzione dell'app mobile
3. (Facoltativo, solo per Android) Configurazione dello scambio di informazioni con Firebase Cloud Messaging

   È consigliabile eseguire questo passaggio per garantire l'invio tempestivo dei comandi ai dispositivi mobili e la sincronizzazione forzata quando vengono modificate le impostazioni dei criteri.

Preparazione di Kaspersky Security Center Web Console e Cloud Console per la distribuzione

Questa sezione fornisce istruzioni sulla preparazione di Kaspersky Security Center Web Console e Cloud Console per la distribuzione.

Configurazione di Administration Server per la connessione dei dispositivi mobili

Affinché i dispositivi mobili possano connettersi ad Administration Server, è necessario definire le impostazioni di connessione dei dispositivi mobili nelle proprietà di Administration Server prima di installare l'app Kaspersky Endpoint Security for Android o l'app Kaspersky Security for iOS nei dispositivi mobili.

Per definire le impostazioni di Administration Server per la connessione dei dispositivi mobili:

1. Avviare Mobile Device Management in Administration Server.

   È possibile avviare Mobile Device Management durante la configurazione iniziale di Administration Console basata su MMC di Kaspersky Security Center (durante l'esecuzione dell'Avvio rapido guidato) o successivamente visualizzando la cartella Mobile Device Management in Administration Console.

2. Fare clic su **Impostazioni** ( ) nella finestra principale di Kaspersky Security Center Web Console o Cloud Console.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

3. Configurare le porte di Administration Server che verranno utilizzate dai dispositivi mobili:

   a. Selezionare la sezione **Porte aggiuntive**.

   b. Abilitare l'interruttore **Apri porta per i dispositivi mobili**.

   c. Nel campo **Porta per la sincronizzazione del dispositivo mobile** specificare la porta tramite la quale i dispositivi mobili si connetteranno all'Administration Server.

      Per impostazione predefinita, viene utilizzata la porta 13292.

      Se l'interruttore **Apri porta per i dispositivi mobili** è deselezionato o è specificata una porta di connessione errata, i dispositivi mobili non saranno in grado di connettersi all'Administration Server.

   d. Nel campo **Porta per l'attivazione del dispositivo mobile** specificare la porta che verrà utilizzata dai dispositivi mobili per la connessione ad Administration Server per l'attivazione dell'app mobile.

      Per impostazione predefinita, viene utilizzata la porta 17100.

Se si specifica una porta di connessione errata, gli utenti dei dispositivi mobili non saranno in grado di attivare l'app mobile utilizzando Administration Server.

4. Se necessario, modificare il certificato che verrà utilizzato dai dispositivi mobili per connettersi ad Administration Server.

   Per impostazione predefinita, Administration Server utilizza il certificato creato durante l'installazione di Administration Server. Se si desidera, sostituire il certificato emesso tramite Administration Server con un altro certificato o riemettere il certificato emesso tramite Administration Server.

   Per modificare il certificato*:*

   a. Selezionare la sezione **Certificati**.

   b. Definire le impostazioni richieste.

      Per informazioni dettagliate sui certificati, fare riferimento alla *Guida di Kaspersky Security Center*.

5. Fare clic sul pulsante **Salva** per salvare le modifiche apportate alle impostazioni e chiudere la finestra delle proprietà di Administration Server.

Dopo aver configurato le impostazioni di connessione dei dispositivi mobili, è possibile installare l'app Kaspersky Endpoint Security for Android o l'app Kaspersky Security for iOS nei dispositivi mobili e connetterli ad Administration Server utilizzando le impostazioni specificate.

Creazione di un gruppo di amministrazione

I criteri di gruppo vengono utilizzati per eseguire la configurazione centralizzata delle app Kaspersky Endpoint Security for Android e Kaspersky Security for iOS installate nei dispositivi mobili degli utenti.

Per applicare un criterio a un gruppo di dispositivi, è consigliabile creare un gruppo distinto per tali dispositivi in **Dispositivi gestiti** prima di installare le app mobili nei dispositivi degli utenti.

Dopo la creazione di un gruppo di amministrazione, è consigliabile configurare l'opzione per l'assegnazione automatica dei dispositivi in cui si desidera installare le app a questo gruppo. Configurare quindi le impostazioni comuni a tutti i dispositivi utilizzando un criterio di gruppo.

Per creare un gruppo di amministrazione:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **GERARCHIA DEI GRUPPI**.

2. Nella struttura dei gruppi di amministrazione selezionare il gruppo di amministrazione che dovrà includere il nuovo gruppo di amministrazione.

3. Fare clic sul pulsante **Aggiungi**.

4. Nella finestra **Nome del nuovo gruppo di amministrazione** visualizzata inserire un nome per il gruppo, quindi fare clic sul pulsante **Aggiungi**.

Nella gerarchia dei gruppi di amministrazione viene visualizzato un nuovo gruppo di amministrazione con il nome specificato.

Creazione di una regola per l'assegnazione automatica di un dispositivo ai gruppi di amministrazione

Quando l'app Kaspersky Endpoint Security for Android o l'app Kaspersky Security for iOS viene installata nei dispositivi mobili, questi ultimi vengono visualizzati nella pagina **INDIVIDUAZIONE E DISTRIBUZIONE** > **DISPOSITIVI NON ASSEGNATI** di Kaspersky Security Center Web Console o Cloud Console. Per gestire i nuovi dispositivi connessi, è possibile spostarli manualmente in un gruppo di amministrazione o creare una regola per assegnarli automaticamente ai gruppi di amministrazione.

Per creare una regola per l'assegnazione automatica dei dispositivi mobili ai gruppi di amministrazione:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **INDIVIDUAZIONE E DISTRIBUZIONE** > **DISTRIBUZIONE E ASSEGNAZIONE** > **REGOLE DI SPOSTAMENTO**.
2. Nella finestra **Nuova regola** visualizzata fare clic sul pulsante **Aggiungi**.
3. Nel campo **Nome regola** specificare il nome della regola.
4. Nel campo **Gruppo di amministrazione** selezionare il gruppo di amministrazione al quale devono essere assegnati i dispositivi mobili dopo l'installazione dell'app.
5. Nella sezione **Applica regola** selezionare **Esegui una volta per ciascun dispositivo**.
6. Selezionare la casella di controllo **Sposta solo dispositivi non aggiunti a un gruppo di amministrazione** per impedire lo spostamento dei dispositivi mobili assegnati ad altri gruppi di amministrazione al momento dell'applicazione della regola.
7. Selezionare la casella di controllo **Abilita regola** per applicare la regola subito dopo averla creata.

   È possibile abilitare la regola in un secondo momento utilizzando l'interruttore nella pagina **REGOLE DI SPOSTAMENTO**.
8. Selezionare **CONDIZIONI DELLE REGOLE** > **Applicazioni** e procedere come segue:

   a. Abilitare l'interruttore **Versione del sistema operativo**.

   b. Nell'elenco dei sistemi operativi visualizzato selezionare **Android** o **iOS**.

   La regola verrà applicata ai dispositivi corrispondenti. Per creare una regola è necessario specificare almeno una condizione.
9. Fare clic su **Salva** per creare la regola.

La nuova regola creata viene visualizzata nella pagina **REGOLE DI SPOSTAMENTO**. In base alla regola, Kaspersky Security Center assegnerà tutti i nuovi dispositivi connessi al gruppo di amministrazione selezionato.

Per informazioni dettagliate sulla gestione dei gruppi di amministrazione e sulle azioni con i dispositivi non assegnati:

- Se si utilizza Kaspersky Security Center Web Console, fare riferimento alla *Guida di Kaspersky Security Center*.
- Se si utilizza Kaspersky Security Center Cloud Console, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

Distribuzione dei plug-in di amministrazione

Per gestire i dispositivi mobili in Kaspersky Security Center Web Console, è necessario installare i seguenti plug-in di amministrazione:

- Plug-in di Kaspersky Security for Mobile (Devices)
- Plug-in di Kaspersky Security for Mobile (Policies)

Se si utilizza Kaspersky Security Center Cloud Console, non è necessario installare i plug-in di amministrazione. È sufficiente creare un account in Kaspersky Security Center Cloud Console. Per ulteriori informazioni sulla creazione di un account, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

Per installare i plug-in di amministrazione è possibile utilizzare i seguenti metodi:

- Tramite l'Avvio rapido guidato di Kaspersky Security Center Web Console.

  Kaspersky Security Center Web Console richiede automaticamente di eseguire l'Avvio rapido guidato dopo l'installazione di Administration Server alla prima connessione. È inoltre possibile avviare manualmente l'Avvio rapido guidato in qualsiasi momento.

  Per ulteriori informazioni sull'Avvio rapido guidato per Kaspersky Security Center, fare riferimento alla *Guida di Kaspersky Security Center*.

- Tramite l'elenco dei pacchetti di distribuzione disponibili in Kaspersky Security Center Web Console.

  L'elenco dei pacchetti di distribuzione disponibili viene aggiornato automaticamente dopo il rilascio di nuove versioni delle applicazioni Kaspersky.

- Scaricare i pacchetti di distribuzione da un'origine esterna e aggiungere i plug-in di amministrazione a Kaspersky Security Center Web Console.

  I pacchetti di distribuzione dei plug-in di amministrazione possono ad esempio essere scaricati sul sito Web Kaspersky.

Installazione dei plug-in di amministrazione dall'elenco dei pacchetti di distribuzione disponibili

Per installare i plug-in di amministrazione:

1. Nella finestra principale di Kaspersky Security Center Web Console selezionare **IMPOSTAZIONI DELLA CONSOLE** > **PLUG-IN WEB**.
2. Fare clic sul pulsante **Aggiungi**.

   Si aprirà l'elenco delle versioni aggiornate delle applicazioni Kaspersky.
3. Installare i plug-in di amministrazione:

   a. Nell'elenco delle applicazioni disponibili fare clic sulla sezione **Dispositivi mobili** per espanderla.

   b. Selezionare **Kaspersky Security for Mobile (Devices)**, quindi fare clic su **Installa plug-in**.

   c. Selezionare **Kaspersky Security for Mobile (Policies)**, quindi fare clic su **Installa plug-in**.

I pacchetti di distribuzione verranno scaricati e i plug-in saranno installati. Quando ciascun plug-in viene installato e aggiunto a Kaspersky Security Center Web Console, viene visualizzata una finestra di conferma.

Installazione dei plug-in di amministrazione dal pacchetto di distribuzione

È possibile scaricare il pacchetto di distribuzione dal sito Web di Kaspersky.

Per installare il plug-in di Kaspersky Security for Mobile (Devices) dal pacchetto di distribuzione:

1. Copiare i file `plugin.zip` e `signature.txt` dall'archivio `on_prem_ksm_devices_xx.x.x.x.zip` del pacchetto di distribuzione alla workstation dell'amministratore.
2. Nella finestra principale di Kaspersky Security Center Web Console selezionare **IMPOSTAZIONI DELLA CONSOLE** > **PLUG-IN WEB**.
3. Fare clic su **Aggiungi da file**.
4. Nella finestra **Aggiungi da file** visualizzata fare clic su **Carica file ZIP**, quindi cercare il file `plugin.zip`.
5. Fare clic su **Carica firma**, quindi cercare il file `signature.txt`.
6. Fare clic sul pulsante **Aggiungi**.

   Il plug-in di Kaspersky Security for Mobile (Devices) verrà installato e aggiunto a Kaspersky Security Center Web Console.

Per installare il plug-in di Kaspersky Security for Mobile (Policies) dal pacchetto di distribuzione:

1. Copiare i file `plugin.zip` e `signature.txt` dall'archivio `on_prem_ksm_policies_xx.x.x.x.zip` del pacchetto di distribuzione alla workstation dell'amministratore.
2. Nella finestra principale di Kaspersky Security Center Web Console selezionare **IMPOSTAZIONI DELLA CONSOLE** > **PLUG-IN WEB**.
3. Fare clic su **Aggiungi da file**.
4. Nella finestra **Aggiungi da file** visualizzata fare clic su **Carica file ZIP**, quindi cercare il file `plugin.zip`.
5. Fare clic su **Carica firma**, quindi cercare il file `signature.txt`.
6. Fare clic sul pulsante **Aggiungi**.

   Il plug-in di Kaspersky Security for Mobile (Policies) verrà installato e aggiunto a Kaspersky Security Center Web Console.

È possibile assicurarsi che i plug-in di amministrazione siano stati installati visualizzando l'elenco dei plug-in installati nella pagina **IMPOSTAZIONI DELLA CONSOLE** > **PLUG-IN WEB**.

Distribuzione dell'app mobile

Per gestire i dispositivi mobili in Kaspersky Security Center Web Console o Cloud Console, è necessario distribuire l'app Kaspersky Endpoint Security for Android o l'app Kaspersky Security for iOS nei dispositivi mobili. È possibile distribuire le app nei dispositivi mobili utilizzando Kaspersky Security Center Web Console o Cloud Console.

Distribuzione dell'app mobile tramite Kaspersky Security Center Web Console o Cloud Console

L'app mobile viene distribuita nei dispositivi mobili degli utenti i cui account utente sono stati aggiunti a Kaspersky Security Center. Per ulteriori informazioni sugli account utente in Kaspersky Security Center:

- Se si utilizza Kaspersky Security Center Web Console, fare riferimento alla *Guida di Kaspersky Security Center*.
- Se si utilizza Kaspersky Security Center Cloud Console, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

È possibile utilizzare il plug-in di Kaspersky Security for Mobile (Devices) per installare l'app da Kaspersky Security Center Web Console e Cloud Console inviando un collegamento per l'installazione a un dispositivo mobile.

- In un dispositivo Android l'utente riceve un collegamento a Google Play per scaricare l'app Kaspersky Endpoint Security for Android. L'app può essere installata seguendo la procedura di installazione standard nella piattaforma Android. Dopo l'installazione dell'app, l'utente deve fornire le autorizzazioni necessarie.

  Alcuni dispositivi Huawei e Honor non dispongono dei servizi Google e quindi dell'accesso alle app in Google Play. Se alcuni utenti di dispositivi Huawei e Honor non possono installare l'app da Google Play, dovrebbero ricevere indicazione di installare l'app da Huawei App Gallery.

- In un dispositivo iOS l'utente riceve un collegamento all'App Store per scaricare l'app Kaspersky Security for iOS. L'app può essere installata seguendo la procedura di installazione standard nella piattaforma iOS.

  Prima di collegare un dispositivo iOS, inviare l'indirizzo di Kaspersky Security Center all'utente del dispositivo per migliorare la sicurezza della connessione. L'utente vedrà questo indirizzo durante l'installazione dell'app e potrà annullare la connessione se l'indirizzo visualizzato non corrisponde all'indirizzo inviato.

Il collegamento contiene i seguenti dati:

- Impostazioni di sincronizzazione di Kaspersky Security Center
- Certificato generale

Per distribuire l'app in un dispositivo mobile:

1. Avviare la Connessione guidata nuovo dispositivo mobile:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**, quindi fare clic su **Aggiungi**.
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **UTENTI E RUOLI** > **UTENTI**. Fare clic sul nome dell'utente o del gruppo di utenti a cui si desidera inviare il collegamento per la connessione di un dispositivo mobile, quindi selezionare **DISPOSITIVI.** Fare clic su **Aggiungi dispositivo mobile**. In tal caso, ignorare il passaggio 3.

   Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Selezionare il sistema operativo dei dispositivi che si desidera aggiungere:

   - **Android**
   - **iOS e iPadOS**

3. Selezionare gli utenti e i gruppi di utenti a cui si desidera inviare il collegamento per la connessione di un dispositivo mobile.

4. Selezionare gli indirizzi e-mail a cui inviare il collegamento:

   - **Tutti gli indirizzi e-mail**
   - **Indirizzo e-mail principale**
   - **Indirizzo e-mail alternativo**
   - **Un altro indirizzo e-mail**

     Se si seleziona questa opzione, specificare l'indirizzo e-mail di seguito.

5. Viene visualizzato il riepilogo del collegamento.

   Assicurarsi che tutti i parametri del collegamento siano corretti, quindi fare clic su **Invia**.

6. Verrà visualizzata una finestra con la conferma dell'invio del collegamento per l'aggiunta di un dispositivo mobile.

   Fare clic su **OK** per terminare la procedura guidata.

Quando l'utente installa l'app Kaspersky Endpoint Security for Android o l'app Kaspersky Security for iOS, il relativo dispositivo verrà visualizzato nella scheda **DISPOSITIVI** > **MOBILI** > **DISPOSITIVI** di Web Console o Cloud Console. Dopo l'installazione dell'app nei dispositivi mobili degli utenti, sarà possibile configurare le impostazioni per i dispositivi e le app utilizzando i criteri di gruppo. Sarà inoltre possibile inviare comandi ai dispositivi mobili (solo per Android) per la protezione dei dati in caso di furto o smarrimento dei dispositivi.

Attivazione dell'app mobile

In Kaspersky Security Center, la licenza può coprire vari gruppi di funzionalità. Per garantire la piena operatività dell'app Kaspersky Endpoint Security for Android e dell'app Kaspersky Security for iOS, la licenza di Kaspersky Security Center acquistata dall'organizzazione deve offrire la funzionalità **Mobile Device Management**. La funzionalità **Mobile Device Management** è progettata per la connessione dei dispositivi mobili a Kaspersky Security Center e per la relativa gestione.

Per informazioni dettagliate sul licensing di Kaspersky Security Center e sulle opzioni di licenza*:*

- Se si utilizza Kaspersky Security Center Web Console, fare riferimento alla *Guida di Kaspersky Security Center*.
- Se si utilizza Kaspersky Security Center Cloud Console, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

L'attivazione dell'app Kaspersky Endpoint Security for Android o dell'app Kaspersky Security for iOS in un dispositivo mobile viene eseguita fornendo all'app informazioni di licenza valide. Le informazioni sulla licenza vengono distribuite al dispositivo mobile insieme al criterio quando il dispositivo viene sincronizzato con Kaspersky Security Center.

Se l'attivazione dell'app mobile non viene completata entro 30 giorni dal momento dell'installazione nel dispositivo mobile, l'app passerà automaticamente alla modalità con funzionalità limitate. In questa modalità, la maggior parte dei componenti dell'app non è operativa. Quando passa alla modalità con funzionalità limitate, l'app smette di eseguire la sincronizzazione automatica con Kaspersky Security Center. Pertanto, se l'attivazione dell'app non viene completata entro 30 giorni dall'installazione, l'utente deve sincronizzare manualmente il dispositivo con Kaspersky Security Center.

Se Kaspersky Security Center non è distribuito nell'organizzazione o non è accessibile ai dispositivi mobili, gli utenti possono attivare manualmente l'app mobile nei propri dispositivi.

Per attivare l'app mobile:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Licenze**.

3. Utilizzare l'elenco a discesa per selezionare la chiave di licenza desiderata dall'archivio delle chiavi di Administration Server.

   I dettagli della chiave di licenza sono visualizzati nei campi di seguito.

   > È possibile sostituire la chiave di attivazione esistente nel dispositivo mobile se è diversa da quella selezionata nell'elenco a discesa precedente. A tale scopo, selezionare la casella di controllo **Se la chiave nel dispositivo è diversa, sostituisci con questa chiave**.

4. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Concessione delle autorizzazioni necessarie per l'app Kaspersky Endpoint Security for Android

Alcune funzionalità dell'app Kaspersky Endpoint Security for Android richiedono autorizzazioni. Kaspersky Endpoint Security for Android richiede autorizzazioni obbligatorie durante l'installazione, nonché dopo l'installazione e prima di utilizzare le singole funzionalità dell'app. È impossibile installare Kaspersky Endpoint Security for Android senza concedere le autorizzazioni obbligatorie.

In determinati dispositivi (ad esempio Huawei, Meizu e Xiaomi) è necessario aggiungere manualmente Kaspersky Endpoint Security for Android all'elenco delle app eseguite all'avvio del sistema operativo, nelle impostazioni del dispositivo. Se l'app non viene aggiunta all'elenco, Kaspersky Endpoint Security for Android interrompe l'esecuzione di tutte le funzioni in seguito al riavvio del dispositivo mobile.

Nei dispositivi con Android 11 o versioni successive è necessario disabilitare l'impostazione di sistema **Rimuovi le autorizzazioni se l'app non viene utilizzata**. In caso contrario, dopo che l'app non viene utilizzata per alcuni mesi il sistema ripristina automaticamente le autorizzazioni che l'utente ha concesso all'app.

Autorizzazioni richieste dall'app Kaspersky Endpoint Security for Android

Autorizzazione	Funzione dell'app
Telefono (richiesta solo per Android 5.0–9.X)	Connessione a Kaspersky Security Center (ID dispositivo)
Memoria (obbligatorio)	Anti-Virus
Accesso per gestire tutti i file	Anti-Virus (solo per Android 11 o versioni successive)
Dispositivi Bluetooth nelle vicinanze (per Android 12 o versioni successive)	Limita l'uso del Bluetooth
Amministratore dispositivo (obbligatoria)	Antifurto—blocco del dispositivo (solo per Android 5.0–6.X)
	Antifurto—foto utente con la fotocamera anteriore Sebbene l'acquisizione di foto utente non sia supportata in Kaspersky Security Center Web Console e Cloud Console, l'app Kaspersky Endpoint Security for Android richiede questa autorizzazione in modo che possa essere gestita da tutte le console di Kaspersky Security Center.
	Antifurto—riproduzione di un allarme
	Antifurto—ripristino completo
	Protezione tramite password
	Protezione dalla rimozione dell'app
	Installazione del certificato di sicurezza
	Controllo app
	Limitazione dell'utilizzo di fotocamera, Bluetooth e Wi-Fi
Fotocamera	Antifurto—foto utente con la fotocamera anteriore Sebbene l'acquisizione di foto utente non sia supportata in Kaspersky Security Center Web Console e Cloud Console, l'app Kaspersky Endpoint Security for Android richiede questa autorizzazione in modo che possa essere gestita da tutte le console di Kaspersky Security Center. Nei dispositivi che eseguono Android 11.0 o versioni successive, l'utente deve concedere l'autorizzazione "Durante l'utilizzo dell'app" quando richiesto.

Posizione	Antifurto—localizzazione del dispositivo Nei dispositivi che eseguono Android 10.0 o versioni successive l'utente deve concedere l'autorizzazione "Sempre" quando richiesto.
Accessibilità	Antifurto—blocco del dispositivo (solo per Android 7.0 o versione successiva)
	Protezione Web
	Controllo app
	Protezione dalla rimozione dell'app (solo per Android 7.0 o versione successiva)
	Visualizzazione degli avvisi di Kaspersky Endpoint Security for Android (solo per Android 10.0 o versione successiva)
	Limitazione dell'utilizzo della fotocamera (solo per Android 11 o versioni successive)

Gestione dei certificati

I certificati mobili vengono utilizzati allo scopo di identificare gli utenti dei dispositivi mobili in Administration Server.

Kaspersky Security Center Web Console e Cloud Console consentono di eseguire le seguenti azioni con i certificati mobili dell'utente:

- Visualizzare i certificati e i relativi stati.
- Creare nuovi certificati.
- Rinnovare i certificati in scadenza.
- Eliminare i certificati.

Per ulteriori informazioni sui certificati di Kaspersky Security Center:

- Se si utilizza Kaspersky Security Center Web Console, fare riferimento alla *Guida di Kaspersky Security Center*.
- Se si utilizza Kaspersky Security Center Cloud Console, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

Visualizzazione dell'elenco dei certificati

Kaspersky Security Center Web Console e Cloud Console consentono di visualizzare i certificati mobili dell'utente applicati, i relativi stati e le proprietà.

Per visualizzare l'elenco dei certificati mobili dell'utente applicati:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILI** > **DISPOSITIVI**.

2. Selezionare **Gestisci certificati**.

Verrà visualizzata la pagina **Certificati mobili** con le informazioni sui certificati mobili dell'utente applicati. È possibile visualizzare i dettagli di un certificato facendo clic su di esso nella colonna **Nome utente**.

Definizione delle impostazioni del certificato

È possibile utilizzare Kaspersky Security Center Web Console o Cloud Console per configurare la durata, gli aggiornamenti automatici e la protezione tramite password dei certificati mobili.

Per definire le impostazioni del certificato mobile:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILI** > **DISPOSITIVI**.

2. Selezionare **Gestisci certificati**.

3. Selezionare **Impostazioni del certificato**.

4. Nella finestra **Genera certificati mobili** visualizzata è possibile configurare le seguenti impostazioni:

   - **Periodo di validità del certificato (giorni)**

     Periodo di validità del certificato in giorni. La durata predefinita di un certificato è di 365 giorni. Allo scadere di tale periodo, il dispositivo mobile non sarà in grado di connettersi ad Administration Server.

   - **Riemetti allo scadere del certificato tra (giorni)**

     Il numero di giorni rimanenti prima della scadenza del certificato corrente durante i quali Administration Server deve emettere un nuovo certificato. Se ad esempio il valore del campo è 4, Administration Server emette un nuovo certificato quattro giorni prima della scadenza del certificato corrente. Il valore predefinito è 1.

   - **Riemetti automaticamente il certificato, se possibile**

     Se possibile, i certificati verranno riemessi automaticamente. Se questa opzione è disabilitata, i certificati devono essere riemessi manualmente quando scadono. Per impostazione predefinita, questa opzione è disabilitata.

   - **Richiedi password durante l'installazione del certificato**

     All'utente verrà richiesta una password quando il certificato viene installato in un dispositivo mobile. La password viene utilizzata una sola volta, durante l'installazione del certificato nel dispositivo mobile. La password verrà generata automaticamente dall'Administration Server e inviata all'utente tramite e-mail. È possibile specificare la lunghezza della password nel campo **Lunghezza della password**.

5. Fare clic su **Salva** per applicare le modifiche e chiudere la finestra.

Le impostazioni specificate verranno utilizzate da Kaspersky Security Center per la creazione, l'aggiornamento e la protezione dei certificati mobili.

Creazione di un certificato

È possibile creare certificati mobili in Kaspersky Security Center Web Console e Cloud Console allo scopo di identificare gli utenti dei dispositivi mobili.

Per creare un certificato mobile:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILI** > **DISPOSITIVI**.

2. Selezionare **Gestisci certificati**.

3. Nella finestra **Certificati mobili** visualizzata fare clic su **Aggiungi** per avviare la **Creazione guidata certificato mobile**. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Selezionare gli utenti o i gruppi di utenti di cui si desidera gestire i dispositivi mobili con un nuovo certificato.

5. Specificare i **Parametri di pubblicazione**:

   - Se si desidera inviare una notifica agli utenti sul nuovo certificato, selezionare la casella di controllo **Informa l'utente del nuovo certificato**.

   - Se si desidera consentire l'utilizzo di un certificato più volte sullo stesso dispositivo, selezionare la casella di controllo **Consenti l'utilizzo di un certificato più volte nello stesso dispositivo (solo per i dispositivi in cui è installato Kaspersky Endpoint Security for Android)**.

6. Selezionare il **Tipo di autenticazione**:

   - Selezionare **Credenziali (nome utente o login del dominio)** se si desidera che gli utenti accedano al certificato utilizzando le proprie credenziali.

   - Selezionare **Password monouso** se si desidera che gli utenti accedano al certificato utilizzando una password monouso.

     Questa opzione è disponibile se non è stata selezionata la casella di controllo **Consenti l'utilizzo di un certificato più volte nello stesso dispositivo (solo per i dispositivi in cui è installato Kaspersky Endpoint Security for Android)** nel passaggio precedente.

   - Selezionare **Password** se si desidera che gli utenti accedano al certificato utilizzando una password.

     Questa opzione è disponibile se è stata selezionata la casella di controllo **Consenti l'utilizzo di un certificato più volte nello stesso dispositivo (solo per i dispositivi in cui è installato Kaspersky Endpoint Security for Android)** nel passaggio precedente.

7. Specificare il metodo di invio del certificato nel campo **Invio del certificato**:

   - Se è stato selezionato **Password monouso** nel passaggio precedente, selezionare una delle seguenti opzioni:

     - Se si desidera inviare la password tramite e-mail, selezionare **Informa l'utente tramite e-mail**.

       Quindi selezionare l'indirizzo e-mail da utilizzare o selezionare **Un altro indirizzo e-mail** per specificare un altro indirizzo e-mail.

     - Se si desidera inviare una notifica agli utenti sulla password con altri metodi, selezionare **Mostra la password al termine della procedura guidata**.

   - Se è stato selezionato **Credenziali (nome utente o login del dominio)** nel passaggio precedente, selezionare l'indirizzo e-mail da utilizzare o selezionare **Un altro indirizzo e-mail** per specificare un altro indirizzo e-mail.

8. Verrà visualizzato il riepilogo del certificato.

   Assicurarsi che tutti i parametri siano corretti, quindi fare clic su **Crea**.

Come risultato, la **Creazione guidata certificato mobile** crea un certificato che gli utenti possono installare nei propri dispositivi mobili. Il certificato diventa disponibile dopo la successiva sincronizzazione dei dispositivi mobili con Kaspersky Security Center.

Per ulteriori informazioni sulla creazione di certificati e sulla configurazione delle regole per emetterli:

- Se si utilizza Kaspersky Security Center Web Console, fare riferimento alla *Guida di Kaspersky Security Center*.
- Se si utilizza Kaspersky Security Center Cloud Console, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

Rinnovo di un certificato

Se uno dei certificati mobili applicati sta per scadere, è possibile rinnovarlo utilizzando Kaspersky Security Center Web Console o Cloud Console.

Per rinnovare un certificato mobile:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILI** > **DISPOSITIVI**.
2. Selezionare **Gestisci certificati**.
3. Selezionare il certificato che si desidera rinnovare, quindi fare clic su **Riemetti**.

Lo stato del certificato diventa **Il certificato è stato riemesso**.

Eliminazione di un certificato

È possibile eliminare i certificati mobili utilizzando Kaspersky Security Center Web Console o Cloud Console.

Se si elimina un certificato mobile, il dispositivo non può più sincronizzarsi con Administration Server e non può essere gestito tramite Kaspersky Security Center. Per ricominciare a gestire il dispositivo mobile, sarà necessario reinstallare l'app Kaspersky Endpoint Security for Android.

Per eliminare un certificato mobile:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILI** > **DISPOSITIVI**.
2. Selezionare **Gestisci certificati**.
3. Selezionare il certificato che si desidera eliminare, quindi fare clic su **Elimina**.

Il certificato viene eliminato e rimosso dall'elenco dei certificati.

Scambio di informazioni con Firebase Cloud Messaging

Kaspersky Endpoint Security for Android utilizza il servizio FCM (Firebase Cloud Messaging) per garantire l'invio tempestivo dei comandi ai dispositivi mobili e la sincronizzazione forzata quando le impostazioni dei criteri vengono modificate.

Per utilizzare il servizio Firebase Cloud Messaging, è necessario definire le impostazioni del servizio in Kaspersky Security Center Web Console o Cloud Console.

Per abilitare Firebase Cloud Messaging in Kaspersky Security Center Web Console o Cloud Console:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **SINCRONIZZAZIONE DEI DISPOSITIVI ANDROID**.

   Verrà aperta la finestra **Sincronizzazione dei dispositivi Android**.

2. Nei campi **ID mittente** e **Chiave del server** specificare le impostazioni di Firebase Cloud Messaging: SENDER_ID e chiave API.

Firebase Cloud Messaging è abilitato.

Per ottenere un ID mittente e la chiave server:

1. Registrarsi al portale Google.
2. Passare a Google Cloud Platform.
3. Creare un nuovo progetto.

   Attendere la creazione del progetto.
4. Trovare il SENDER_ID attinente del progetto.
5. Abilitare Google Firebase Cloud Messaging per Android.
6. Seguire le istruzioni visualizzate per creare le credenziali.
7. Recuperare la chiave API dalle proprietà delle credenziali appena create.

Per informazioni dettagliate sulle operazioni in Google Cloud Platform, fare riferimento alla relativa documentazione.

Adesso si dispone di un **ID mittente** e di una **Chiave del server** per configurare le impostazioni di Firebase Cloud Messaging.

Se le impostazioni di Firebase Cloud Messaging non sono definite, i comandi nel dispositivo mobile e le impostazioni dei criteri verranno inviati quando il dispositivo viene sincronizzato con Kaspersky Security Center in base alla pianificazione impostata nel criterio (ad esempio ogni 24 ore). In altre parole, i comandi e le impostazioni dei criteri verranno inviati con un ritardo.

Allo scopo di supportare la funzionalità principale del prodotto, si accetta di fornire automaticamente il servizio Firebase Cloud Messaging con l'ID univoco dell'installazione dell'app (ID istanza) e i seguenti dati:

- Informazioni sul software installato: versione dell'app, ID dell'app, versione della build dell'app, nome del pacchetto dell'app.
- Informazioni sul computer in cui è installato il software: versione del sistema operativo, ID dispositivo, versione dei servizi Google.

- Informazioni su FCM: ID dell'app in FCM, ID utente di FCM, versione del protocollo.

I dati vengono trasmessi ai servizi Firebase tramite una connessione sicura. L'accesso e la protezione delle informazioni sono disciplinati dai relativi termini di utilizzo dei servizi Firebase: Firebase Data Processing and Security Terms (Termini di elaborazione e sicurezza dei dati di Firebase), Privacy e sicurezza in Firebase.

Per impedire lo scambio di informazioni con il servizio Firebase Cloud Messaging:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **SINCRONIZZAZIONE DEI DISPOSITIVI ANDROID**.

   Verrà aperta la finestra **Sincronizzazione dei dispositivi Android**.

2. Fare clic su **Reimposta**.

3. Nella finestra visualizzata fare clic sul pulsante **OK** per confermare la reimpostazione.

Le impostazioni di Firebase Cloud Messaging vengono cancellate.

Gestione dei dispositivi mobili in Kaspersky Security Center Web Console e Cloud Console

È possibile gestire i dispositivi mobili in Kaspersky Security Center Web Console e Cloud Console utilizzando criteri di gruppo e inviando comandi ai dispositivi mobili (solo per Android).

Per gestire i dispositivi mobili in Kaspersky Security Center Web Console, è necessario installare i plug-in di amministrazione.

Connessione dei dispositivi mobili a Kaspersky Security Center

Per gestire un dispositivo mobile utilizzando Kaspersky Security Center Web Console o Cloud Console, il dispositivo deve essere connesso a Kaspersky Security Center. È possibile visualizzare l'elenco dei dispositivi mobili connessi a Kaspersky Security Center nella scheda **DISPOSITIVI** > **MOBILI** > **DISPOSITIVI** di Web Console o Cloud Console.

Prima di collegare un dispositivo iOS, inviare l'indirizzo di Kaspersky Security Center all'utente del dispositivo per migliorare la sicurezza della connessione. L'utente vedrà questo indirizzo durante l'installazione dell'app e potrà annullare la connessione se l'indirizzo visualizzato non corrisponde all'indirizzo inviato.

Per connettere un dispositivo mobile a Kaspersky Security Center:

1. Avviare la Connessione guidata nuovo dispositivo mobile:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**, quindi fare clic su **Aggiungi**.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **UTENTI E RUOLI** > **UTENTI**. Fare clic sul nome dell'utente o del gruppo di utenti a cui si desidera inviare il collegamento per la connessione di un dispositivo mobile, quindi selezionare **DISPOSITIVI.** Fare clic su **Aggiungi dispositivo mobile**. In tal caso, ignorare il passaggio 3.

Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

2. Selezionare il sistema operativo dei dispositivi che si desidera aggiungere:

   - **Android**
   - **iOS e iPadOS**

3. Selezionare gli utenti e i gruppi di utenti a cui si desidera inviare il collegamento per la connessione di un dispositivo mobile.

4. Selezionare gli indirizzi e-mail a cui inviare il collegamento:

   - **Tutti gli indirizzi e-mail**
   - **Indirizzo e-mail principale**
   - **Indirizzo e-mail alternativo**
   - **Un altro indirizzo e-mail**

     Se si seleziona questa opzione, specificare l'indirizzo e-mail di seguito.

5. Viene visualizzato il riepilogo del collegamento.

   Assicurarsi che tutti i parametri del collegamento siano corretti, quindi fare clic su **Invia**.

6. Verrà visualizzata una finestra con la conferma dell'invio del collegamento per l'aggiunta di un dispositivo mobile.

   Fare clic su **OK** per terminare la procedura guidata.

Quando l'utente installa l'app Kaspersky Endpoint Security for Android o l'app Kaspersky Security for iOS, il dispositivo dell'utente verrà visualizzato nella scheda **DISPOSITIVI** > **MOBILI** > **DISPOSITIVI** di Web Console o Cloud Console.

Spostamento dei dispositivi mobili non assegnati in gruppi di amministrazione

Quando l'app Kaspersky Endpoint Security for Android o l'app Kaspersky Security for iOS viene installata nei dispositivi mobili, questi ultimi vengono visualizzati nella pagina **INDIVIDUAZIONE E DISTRIBUZIONE** > **DISPOSITIVI NON ASSEGNATI** di Kaspersky Security Center Web Console o Cloud Console. Per gestire i nuovi dispositivi connessi, è possibile creare una regola per l'assegnazione automatica ai gruppi di amministrazione o spostarli manualmente in un gruppo di amministrazione.

Per spostare un dispositivo mobile non assegnato in un gruppo di amministrazione:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **INDIVIDUAZIONE E DISTRIBUZIONE** > **DISPOSITIVI NON ASSEGNATI**.

2. Selezionare il dispositivo che si desidera spostare in un gruppo di amministrazione, quindi fare clic su **Sposta nel gruppo**.

3. Nella struttura dei gruppi di amministrazione visualizzata selezionare il gruppo di destinazione in cui spostare il dispositivo.

   È possibile creare un nuovo gruppo di amministrazione selezionando un gruppo esistente, quindi facendo clic su **Aggiungi gruppo figlio**.

4. Fare clic su **Sposta**.

Il dispositivo verrà spostato nel gruppo di amministrazione specificato e verranno applicati i criteri di gruppo.

Invio di comandi ai dispositivi mobili

È possibile inviare comandi ai dispositivi mobili Android per proteggere i dati in un dispositivo mobile smarrito o rubato oppure per eseguire la sincronizzazione forzata di un dispositivo mobile con Kaspersky Security Center.

Non è possibile inviare comandi ai dispositivi iOS.

Sono supportati i seguenti comandi:

- **Blocca dispositivo**

  Il dispositivo mobile è bloccato.

- **Sblocca dispositivo**

  Il dispositivo mobile è sbloccato. Dopo aver sbloccato un dispositivo mobile che esegue Android 5.0 - 6.X, la password di sblocco dello schermo (codice PIN) viene reimpostata su "1234". Dopo aver sbloccato un dispositivo che esegue Android 7.0 o versioni successive, la password di sblocco dello schermo non viene modificata.

- **Ripristina le impostazioni predefinite**

  Tutti i dati vengono eliminati dal dispositivo mobile e viene eseguito il rollback delle impostazioni ai valori predefiniti.

- **Cancella dati aziendali**

  I dati inseriti in un contenitore e l'account e-mail aziendale vengono cancellati dal dispositivo mobile.

- **Localizza dispositivo**

  Il dispositivo viene localizzato e visualizzato su Google Maps. Il fornitore di servizi mobili può applicare una tariffa per l'accesso a Internet.

  Nei dispositivi che eseguono Android 12 o versioni successive, se l'utente ha concesso l'autorizzazione per l'utilizzo della posizione approssimativa, l'app Kaspersky Endpoint Security for Android cerca prima di ottenere la posizione esatta del dispositivo. Se l'operazione non va a buon fine, viene restituita la posizione approssimativa del dispositivo solo se è stata ricevuta non più di 30 minuti prima. In caso contrario, il comando di **Localizza dispositivo** non va a buon fine.

- **Attiva allarme**

  Il dispositivo mobile emette un tono di allarme. L'allarme suona per 5 minuti (o per 1 minuto se la batteria del dispositivo è scarica).

- **Sincronizza dispositivo**

  Il dispositivo mobile viene sincronizzato con Kaspersky Security Center.

L'app Kaspersky Endpoint Security for Android richiede autorizzazioni specifiche per l'esecuzione dei comandi. Durante l'esecuzione della procedura guidata di configurazione iniziale, Kaspersky Endpoint Security for Android richiede all'utente di concedere all'applicazione tutte le autorizzazioni richieste. L'utente può ignorare questi passaggi o disabilitare tali autorizzazioni nelle impostazioni del dispositivo in un momento successivo. In tal caso, non sarà possibile eseguire i comandi.

Nei dispositivi che eseguono Android 10.0 o versioni successive, l'utente deve concedere l'autorizzazione "Sempre" per accedere alla posizione. Nei dispositivi che eseguono Android 11.0 o versioni successive, l'utente deve inoltre concedere l'autorizzazione "Durante l'utilizzo dell'app" per accedere alla fotocamera. In caso contrario, i comandi di Antifurto non funzioneranno. L'utente verrà informato di questa limitazione e gli verrà nuovamente richiesto di concedere il livello di autorizzazioni necessario. Se l'utente seleziona l'opzione "Solo questa volta" per l'autorizzazione relativa alla fotocamera, si ritiene che l'accesso sia concesso dall'app. È consigliabile contattare direttamente l'utente se viene richiesta nuovamente l'autorizzazione relativa alla fotocamera.

Per inviare un comando a un dispositivo mobile:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**.
2. Selezionare il dispositivo a cui si desidera inviare il comando, quindi fare clic su **Controllo** o **Gestisci**.
3. Selezionare il comando richiesto nell'elenco **Comandi disponibili**, quindi fare clic su **OK**.
4. Fare clic su **OK** se viene richiesto di confermare l'operazione.

Il comando specificato verrà inviato al dispositivo mobile e sarà visualizzata la finestra di conferma.

Rimozione dei dispositivi mobili da Kaspersky Security Center

Se non è più necessario gestire un dispositivo mobile, è possibile rimuoverlo da Kaspersky Security Center utilizzando Web Console o Cloud Console.

Per rimuovere un dispositivo mobile da Kaspersky Security Center:

1. Rimuovere l'app mobile dal dispositivo o assicurarsi che l'utente abbia rimosso l'app dal dispositivo necessario.
2. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**.
3. Selezionare il dispositivo mobile da rimuovere, quindi fare clic su **Elimina**.
4. Fare clic su **OK** per confermare l'operazione.

Il dispositivo verrà rimosso da Kaspersky Security Center.

Gestione dei criteri di gruppo

Questa sezione descrive come gestire i criteri di gruppo in Kaspersky Security Center Web Console e Cloud Console.

Criteri di gruppo per la gestione dei dispositivi mobili

Un *criterio di gruppo* è un pacchetto di impostazioni per la gestione dei dispositivi mobili che appartengono a un gruppo di amministrazione e delle app mobili installate nei dispositivi.

È possibile utilizzare un criterio per configurare le impostazioni sia di singoli dispositivi che di un gruppo di dispositivi. Per un gruppo di dispositivi, le impostazioni di amministrazione possono essere configurate nella finestra delle proprietà del criterio di gruppo.

Ogni parametro rappresentato in un criterio dispone di un attributo di "blocco", che indica se è consentita la modifica dell'impostazione nei criteri dei livelli nidificati della gerarchia (per i gruppi nidificati e gli Administration Server secondari) nelle impostazioni locali dell'applicazione.

I valori delle impostazioni configurate nel criterio e nelle impostazioni locali dell'applicazione vengono salvati nell'Administration Server, distribuite ai dispositivi mobili durante la sincronizzazione e salvate nei dispositivi come impostazioni correnti. Se l'utente ha specificato altri valori delle impostazioni che non sono stati "bloccati", durante la successiva sincronizzazione del dispositivo con l'Administration Server i nuovi valori delle impostazioni vengono inviati all'Administration Server e salvati nelle impostazioni locali dell'applicazione invece dei valori specificati in precedenza dall'amministratore.

Per tenere aggiornata la protezione aziendale dei dispositivi mobili Android, è possibile monitorare la conformità dei dispositivi degli utenti con i requisiti di protezione aziendali.

Per ulteriori dettagli sulla gestione dei criteri e dei gruppi di amministrazione in Kaspersky Security Center Web Console e Cloud Console:

- Se si utilizza Kaspersky Security Center Web Console, fare riferimento alla *Guida di Kaspersky Security Center*.
- Se si utilizza Kaspersky Security Center Cloud Console, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

Visualizzazione dell'elenco dei criteri di gruppo

Kaspersky Security Center Web Console e Cloud Console consentono di visualizzare i criteri di gruppo, i relativi stati e le proprietà.

Per visualizzare l'elenco dei criteri di gruppo:

Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**.

Verrà aperto l'elenco dei criteri di gruppo con brevi informazioni sui criteri di gruppo. In questa pagina è possibile creare, modificare, copiare, spostare ed eliminare i criteri di gruppo.

Visualizzazione dei risultati della distribuzione dei criteri

Kaspersky Security Center Web Console e Cloud Console consentono di visualizzare il grafico della distribuzione di un criterio di gruppo e le informazioni su tutti i dispositivi che rientrano in tale criterio.

Per visualizzare i risultati della distribuzione di un criterio di gruppo:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**.

2. Nell'elenco dei criteri di gruppo visualizzato selezionare la casella di controllo accanto al nome del criterio per il quale si desidera visualizzare i risultati della distribuzione, quindi fai clic su **Distribuzione**.

Verrà aperta la pagina dei risultati della distribuzione dei criteri. Questa pagina contiene il riepilogo del criterio, il grafico di distribuzione del criterio e la tabella con le informazioni su tutti i dispositivi che rientrano in tale criterio. È possibile aprire la finestra delle proprietà del criterio facendo clic sul pulsante **Configura criterio**.

Creazione di un criterio di gruppo

Kaspersky Security Center Web Console e Cloud Console consentono di creare criteri di gruppo allo scopo di gestire i dispositivi mobili.

Per creare un criterio di gruppo:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**.

2. Nell'elenco dei criteri di gruppo di Kaspersky Security Center visualizzato fare clic su **Percorso corrente** per selezionare il gruppo di amministrazione per cui si desidera creare un criterio.

   Per impostazione predefinita, il nuovo criterio di gruppo viene applicato al gruppo **Dispositivi gestiti**.

3. Fare clic su **Aggiungi** per avviare la Creazione guidata criteri. Procedere con la procedura guidata utilizzando il pulsante **Avanti**.

4. Selezionare un'app a seconda della piattaforma:

   - **Kaspersky Endpoint Security for Android**
   - **Kaspersky Security for iOS**

5. Digitare il nome del nuovo criterio nel campo **Nome**. Se si specifica il nome di un criterio esistente, al nome del nuovo criterio verrà automaticamente aggiunto (1) alla fine.

6. Selezionare lo stato del criterio:

   - **Attivo**

     La procedura guidata salva il criterio creato nell'Administration Server. Alla successiva sincronizzazione del dispositivo mobile con l'Administration Server, il criterio verrà utilizzato nel dispositivo come criterio attivo.

   - **Inattivo**

     La procedura guidata salva il criterio creato nell'Administration Server come criterio di backup. Questo criterio può essere attivato in futuro dopo un evento specifico. Se necessario, un criterio inattivo può essere impostato come attivo.

     È possibile creare diversi criteri per un'applicazione nel gruppo, ma solo uno può essere attivo. Quando si crea un nuovo criterio attivo, il criterio attivo precedente diventa automaticamente inattivo.

7. È possibile abilitare o disabilitare due opzioni di ereditarietà, **Eredita impostazioni dal criterio padre** e **Forza ereditarietà impostazioni nei criteri figlio**:

   - Se si abilita **Eredita impostazioni dal criterio padre** per un gruppo di amministrazione figlio e si bloccano alcune impostazioni nel criterio padre, non è possibile modificare queste impostazioni nel criterio per il gruppo figlio. È tuttavia possibile modificare le impostazioni che non sono bloccate nel criterio padre.

   - Se si disabilita **Eredita impostazioni dal criterio padre** per un gruppo di amministrazione figlio, è possibile modificare tutte le impostazioni nel gruppo figlio, anche se alcune impostazioni sono bloccate nel criterio padre.

   - Se si abilita **Forza ereditarietà impostazioni nei criteri figlio** nel gruppo di amministrazione padre, viene abilitata l'opzione **Eredita impostazioni dal criterio padre** per ogni criterio figlio. In questo caso, non è possibile disabilitare questa opzione per alcun criterio figlio. Tutte le impostazioni bloccate nel criterio padre vengono ereditate forzatamente nei gruppi figlio e non è possibile modificare queste impostazioni nei gruppi figlio.

   - Nei criteri per il gruppo **Dispositivi gestiti** l'opzione **Eredita impostazioni dal criterio padre** non ha alcun effetto sulle impostazioni, perché il gruppo **Dispositivi gestiti** non dispone di gruppi upstream, quindi non eredita alcun criterio.

   Per impostazione predefinita, l'opzione **Eredita impostazioni dal criterio padre** è abilitata e l'opzione **Forza ereditarietà impostazioni nei criteri figlio** è disabilitata.

8. Se si desidera, è possibile definire le impostazioni del nuovo criterio creato. A tale scopo, selezionare la scheda **IMPOSTAZIONI APPLICAZIONE**, quindi procedere come descritto nella sezione "Definizione delle impostazioni dei criteri".

   In alternativa, è possibile eseguire questa operazione in seguito.

9. Fare clic su **Salva** per creare il criterio.

Verrà creato un nuovo criterio di gruppo per la gestione dei dispositivi mobili.

Modifica di un criterio di gruppo

Kaspersky Security Center Web Console e Cloud Console consentono di modificare le impostazioni dei criteri di gruppo.

Per modificare un criterio di gruppo:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella finestra delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE**, quindi definire le impostazioni dei criteri come descritto nella sezione "Definizione delle impostazioni dei criteri".

È inoltre possibile configurare le impostazioni generali, l'ereditarietà delle impostazioni, la registrazione e le notifiche degli eventi, i profili criterio e visualizzare la cronologia delle revisioni. Per ulteriori informazioni, fare riferimento alla *Guida di Kaspersky Security Center*.

3. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Copia di un criterio di gruppo

Kaspersky Security Center Web Console e Cloud Console consentono di creare una copia di un criterio di gruppo.

Per creare una copia di un criterio di gruppo:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**.
2. Nell'elenco dei criteri di gruppo visualizzato selezionare la casella di controllo accanto al nome del criterio di cui si desidera creare una copia, quindi fare clic su **Copia**.
3. Nella struttura dei gruppi di amministrazione visualizzata selezionare il gruppo di destinazione in cui creare una copia del criterio.

   È possibile creare un nuovo gruppo di amministrazione selezionando un gruppo esistente, quindi facendo clic su **Aggiungi gruppo figlio**.
4. Fare clic su **Copia**.
5. Fare clic su **OK** per confermare l'operazione.

Nel gruppo di destinazione verrà creata una copia del criterio con lo stesso nome. Lo stato di ogni criterio copiato o spostato nel gruppo di destinazione sarà **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

Se nel gruppo di destinazione esiste già un criterio con un nome identico a quello del criterio appena creato o spostato, al nome del criterio appena creato o spostato viene aggiunto l'indice (<numero di sequenza successivo>), ad esempio: (1).

Spostamento di un criterio in un altro gruppo di amministrazione

Kaspersky Security Center Web Console e Cloud Console consentono di spostare un criterio in un altro gruppo di amministrazione.

Per spostare un criterio in un altro gruppo di amministrazione:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**.

2. Nell'elenco dei criteri di gruppo visualizzato selezionare la casella di controllo accanto al nome del criterio che si desidera spostare in un altro gruppo di amministrazione, quindi fare clic su **Sposta**.

3. Nella struttura dei gruppi di amministrazione visualizzata selezionare il gruppo di destinazione in cui spostare il criterio.

   È possibile creare un nuovo gruppo di amministrazione selezionando un gruppo esistente, quindi facendo clic su **Aggiungi gruppo figlio**.

4. Fare clic su **Sposta**.

5. Fare clic su **OK** per confermare l'operazione.

Il risultato dipende dalle proprietà di ereditarietà dei criteri:

- Se il criterio non è ereditato nel gruppo di origine, verrà spostato nel gruppo di destinazione.
- Se il criterio è ereditato nel gruppo di origine, non verrà spostato. Verrà invece creata una copia di questo criterio nel gruppo di destinazione.

Lo stato di ogni criterio copiato o spostato nel gruppo di destinazione sarà **Inattivo**. È possibile modificare lo stato in **Attivo** in qualsiasi momento.

Se nel gruppo di destinazione esiste già un criterio con un nome identico a quello del criterio appena creato o spostato, al nome del criterio appena creato o spostato viene aggiunto l'indice (<numero di sequenza successivo>), ad esempio: (1).

Eliminazione di un criterio di gruppo

Kaspersky Security Center Web Console e Cloud Console consentono di eliminare i criteri di gruppo.

> È possibile eliminare solo un criterio non ereditato nel gruppo di amministrazione corrente. Se un criterio viene ereditato, è possibile eliminarlo solo nel gruppo di livello superiore per cui è stato creato.

Per eliminare un criterio di gruppo:

1. Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**.

2. Nell'elenco dei criteri di gruppo visualizzato selezionare la casella di controllo accanto al nome del criterio da eliminare, quindi fare clic su **Elimina**.

3. Fare clic su **OK** per confermare l'operazione.

Il criterio di gruppo verrà eliminato.

Definizione delle impostazioni dei criteri

Questa sezione descrive come definire le impostazioni dei criteri di Kaspersky Security Center per la gestione dei dispositivi mobili.

È possibile definire le impostazioni dei criteri durante la creazione o la modifica di un criterio.

Configurazione della protezione anti-virus

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per il rilevamento tempestivo di minacce, virus e altre applicazioni dannose, è necessario configurare la protezione in tempo reale e l'esecuzione automatica delle scansioni virus.

Kaspersky Endpoint Security for Android rileva i seguenti tipi di oggetti:

- Virus, worm, Trojan e strumenti dannosi
- Adware
- App che possono essere sfruttate da utenti malintenzionati per danneggiare il dispositivo o i dati personali

A causa di limitazioni tecniche, Kaspersky Endpoint Security for Android non può esaminare file con dimensioni pari o superiori a 2 GB. Durante una scansione, l'app ignora i file di grandi dimensioni e non invia una notifica in merito.

Configurazione della protezione in tempo reale

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per configurare Protezione in tempo reale:

1. Aprire la finestra delle proprietà dei criteri:
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.
2. Nella finestra delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Protezione essenziale**.
3. Nella sezione **Anti-Virus** configurare la protezione del file system del dispositivo mobile:
   - Per abilitare la protezione in tempo reale del dispositivo mobile dalle minacce, selezionare la casella di controllo **Abilita la protezione anti-virus in tempo reale**.
   - Specificare il livello di protezione:

- Se si desidera che Kaspersky Endpoint Security for Android esegua la scansione solo delle nuove app e dei nuovi file nella cartella Download, selezionare **Esamina solo le nuove app**.

- Per abilitare la protezione estesa del dispositivo mobile dalle minacce, selezionare **Esamina tutte le app e monitora le azioni relative ai file**.

  Kaspersky Endpoint Security for Android eseguirà la scansione di tutti i file aperti, modificati, spostati, copiati, installati o salvati dall'utente nel dispositivo e di tutte le nuove app mobili installate.

  Nei dispositivi con sistema operativo Android 8.0 o versione successiva, Kaspersky Endpoint Security for Android esamina i file modificati, spostati, installati e salvati dall'utente, nonché le copie dei file. Kaspersky Endpoint Security for Android non esamina i file quando vengono aperti, né i file di origine quando vengono copiati.

- Per abilitare la scansione aggiuntiva delle nuove app prima del primo avvio nel dispositivo dell'utente tramite il servizio cloud Kaspersky Security Network, selezionare la casella **Protezione aggiuntiva di Kaspersky Security Network**.

- Per bloccare adware e app che possono essere sfruttati da utenti malintenzionati per danneggiare il dispositivo o i dati dell'utente, selezionare la casella di controllo **È possibile rilevare adware, autodialer e app utilizzabili da criminali informatici per danneggiare i dati e il dispositivo dell'utente**.

4. Nella sezione **Impostazioni anti-virus** selezionare l'azione da eseguire al rilevamento delle minacce:

   - **Elimina e salva una copia di backup del file in Quarantena**

     Gli oggetti rilevati verranno eliminati automaticamente. All'utente non è richiesto di eseguire azioni aggiuntive. Prima di eliminare un oggetto, Kaspersky Endpoint Security for Android creerà una copia di backup del file e la salverà in Quarantena.

   - **Elimina**

     Gli oggetti rilevati verranno eliminati automaticamente. All'utente non è richiesto di eseguire azioni aggiuntive. Prima di eliminare un oggetto, Kaspersky Endpoint Security for Android visualizzerà una notifica provvisoria sul rilevamento dell'oggetto.

   - **Ignora**

     Se gli oggetti rilevati sono stati ignorati, Kaspersky Endpoint Security for Android avvisa l'utente dei problemi di protezione del dispositivo. Le informazioni sugli oggetti ignorati vengono visualizzate nella sezione **Stato** dell'app. Per ogni minaccia ignorata, l'app propone azioni che l'utente può eseguire per eliminare la minaccia. L'elenco degli oggetti ignorati può ad esempio cambiare se un file dannoso è stato eliminato o spostato. Per ricevere un elenco aggiornato delle minacce, eseguire una scansione completa del dispositivo. Per garantire la protezione ottimale dei dati, eliminare tutti gli oggetti rilevati.

5. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione dell'esecuzione automatica delle scansioni virus in un dispositivo mobile

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per configurare l'esecuzione automatica delle scansioni virus in un dispositivo mobile:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella finestra delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Protezione essenziale**.

3. Per bloccare adware e app che possono essere sfruttati da utenti malintenzionati per danneggiare il dispositivo o i dati dell'utente, selezionare la casella di controllo **È possibile rilevare adware, autodialer e app utilizzabili da criminali informatici per danneggiare i dati e il dispositivo dell'utente** nella sezione **Scansione dispositivo**.

4. Nell'elenco **Azione se viene rilevata una minaccia** selezionare una delle seguenti opzioni:

   - **Elimina e salva una copia di backup del file in Quarantena**

     Gli oggetti rilevati verranno eliminati automaticamente. All'utente non è richiesto di eseguire azioni aggiuntive. Prima di eliminare un oggetto, Kaspersky Endpoint Security for Android creerà una copia di backup del file e la salverà in Quarantena.

   - **Elimina**

     Gli oggetti rilevati verranno eliminati automaticamente. All'utente non è richiesto di eseguire azioni aggiuntive. Prima di eliminare un oggetto, Kaspersky Endpoint Security for Android visualizzerà una notifica provvisoria sul rilevamento dell'oggetto.

   - **Ignora**

     Se gli oggetti rilevati sono stati ignorati, Kaspersky Endpoint Security for Android avvisa l'utente dei problemi di protezione del dispositivo. Le informazioni sugli oggetti ignorati vengono visualizzate nella sezione **Stato** dell'app. Per ogni minaccia ignorata, l'app propone azioni che l'utente può eseguire per eliminare la minaccia. L'elenco degli oggetti ignorati può ad esempio cambiare se un file dannoso è stato eliminato o spostato. Per ricevere un elenco aggiornato delle minacce, eseguire una scansione completa del dispositivo. Per garantire la protezione ottimale dei dati, eliminare tutti gli oggetti rilevati.

   - **Chiedi all'utente**

     L'app Kaspersky Endpoint Security for Android visualizza una notifica che richiede all'utente di scegliere l'azione da eseguire sull'oggetto rilevato: **Ignora** o **Elimina**.

     Quando l'app rileva più oggetti, l'opzione **Chiedi all'utente** consente all'utente del dispositivo di applicare un'azione selezionata a ogni file utilizzando la casella **Applica a tutti**.

Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità al fine di garantire la visualizzazione delle notifiche nei dispositivi mobili che eseguono Android 10.0 o versioni successive. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo. In questo caso Kaspersky Endpoint Security for Android visualizza una finestra di sistema Android che richiede all'utente di scegliere l'azione da eseguire sull'oggetto rilevato: Ignora o Elimina. Per applicare un'azione a più oggetti, è necessario aprire Kaspersky Endpoint Security.

5. Nella sezione **Scansione pianificata** è possibile configurare la scansione completa automatica del file system del dispositivo.

   Selezionare una delle seguenti opzioni:

   - **Disabilitata**

     La scansione del file system del dispositivo non verrà avviata automaticamente.

   - **Dopo l'aggiornamento dei database**

     Il file system del dispositivo verrà esaminato automaticamente a ogni aggiornamento dei database anti-virus.

   - **Giornaliera**

     Il file system del dispositivo verrà esaminato automaticamente ogni giorno.

     Se si seleziona questa opzione, è inoltre possibile specificare l'ora della scansione nel campo **Ora di inizio**.

   - **Settimanalmente ogni**

     Il file system del dispositivo verrà esaminato automaticamente una volta alla settimana.

     Se si seleziona questa opzione, è inoltre possibile selezionare il giorno della settimana in cui si desidera eseguire la scansione utilizzando l'elenco a discesa e specificare l'ora della scansione nel campo **Ora di inizio**.

   In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

6. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione degli aggiornamenti dei database anti-virus

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per configurare gli aggiornamenti dei database anti-virus:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio

che si desidera configurare.

- Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella finestra delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Aggiornamento database**.

3. Nella sezione **Aggiornamento database** configurare la pianificazione degli aggiornamenti automatici dei database nel dispositivo dell'utente.

   Selezionare una delle seguenti opzioni:

   - **Disabilitata**

     Gli aggiornamenti automatici dei database anti-virus verranno disabilitati.

   - **Giornaliera**

     I database anti-virus verranno aggiornati ogni giorno.

     Se si seleziona questa opzione, è inoltre possibile specificare l'ora dell'aggiornamento nel campo **Ora aggiornamento**.

   - **Settimanale**

     I database anti-virus verranno aggiornati una volta alla settimana.

     Se si seleziona questa opzione, è inoltre possibile specificare l'ora dell'aggiornamento nel campo **Ora aggiornamento** e il giorno della settimana in cui si desidera eseguire l'aggiornamento nell'elenco a discesa **Giorno della settimana**.

   In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

4. Nella sezione **Sorgente degli aggiornamenti dei database** specificare la sorgente degli aggiornamenti da cui Kaspersky Endpoint Security for Android riceve e installa gli aggiornamenti dei database anti-virus:

   - **Server Kaspersky**

     Kaspersky Endpoint Security for Android utilizzerà un server di aggiornamento Kaspersky come sorgente degli aggiornamenti per scaricare i database anti-virus nel dispositivo dell'utente.

   - **Administration Server**

     Disponibile solo se si utilizza Kaspersky Security Center Web Console.

     Kaspersky Endpoint Security for Android utilizzerà il repository di Kaspersky Security Center Administration Server come sorgente degli aggiornamenti per scaricare i database anti-virus nel dispositivo dell'utente.

   - **Altra sorgente**

     Kaspersky Endpoint Security for Android utilizzerà un server di terze parti come sorgente degli aggiornamenti per scaricare i database anti-virus nel dispositivo dell'utente.

     Se si seleziona questa opzione, è necessario specificare l'indirizzo di un server HTTP nel campo **Utilizzare un altro server come sorgente degli aggiornamenti per i database anti-virus**.

5. Se si desidera che Kaspersky Endpoint Security for Android scarichi gli aggiornamenti dei database anti-virus in base alla pianificazione quando il dispositivo dell'utente è in roaming, selezionare la casella **Consenti aggiornamento dei database in roaming** nella sezione **Aggiorna i database anti-virus in roaming**.

6. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Definizione delle impostazioni di sblocco del dispositivo

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per mantenere protetto un dispositivo mobile, è necessario configurare l'utilizzo di una password richiesta all'utente quando il dispositivo esce dalla modalità di sospensione.

È possibile imporre restrizioni sull'attività dell'utente nel dispositivo se la password di sblocco è vulnerabile (ad esempio il blocco del dispositivo). È possibile imporre restrizioni utilizzando il componente Controllo conformità.

In alcuni dispositivi Samsung con Android 7.0 o versioni successive, quando l'utente tenta di configurare metodi non supportati per lo sblocco del dispositivo (ad esempio, una password grafica), il dispositivo può essere bloccato se vengono soddisfatte le seguenti condizioni: la protezione dalla rimozione di Kaspersky Endpoint Security for Android è abilitata e sono impostati requisiti per la complessità della password di sblocco dello schermo. Per sbloccare il dispositivo, è necessario inviare un comando speciale al dispositivo.

Per configurare la complessità della password di sblocco del dispositivo:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella finestra delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Protezione essenziale**.

3. Se si desidera che l'app controlli se è impostata o meno una password di sblocco, selezionare la casella **Richiedi di impostare una password di sblocco dello schermo** nella sezione **Protezione tramite password**.

   Se l'applicazione rileva che nel dispositivo non è stata impostata alcuna password di sistema, richiede all'utente di impostarla. La password viene impostata secondo i parametri definiti dall'amministratore.

4. Specificare il numero minimo di caratteri per la password dell'utente.

   Valori possibili: da 4 a 16 caratteri.

   La password dell'utente è composta da 4 caratteri per impostazione predefinita.

Nei dispositivi che eseguono Android 10.0 o versioni successive Kaspersky Endpoint Security risolve i requisiti di complessità della password in uno dei valori di sistema: medio o alto.

I valori per i dispositivi che eseguono Android 10.0 o versioni successive sono determinati dalle seguenti regole:

- Se la lunghezza della password richiesta è compresa tra 1 e 4 simboli, l'app richiede all'utente di impostare una password di complessità media. Deve essere una password numerica (PIN) senza sequenze ripetute o ordinate (ad es. 1234) oppure alfanumerica. Il PIN o la password deve contenere almeno 4 caratteri.
- Se la lunghezza della password richiesta è superiore a 5 simboli, l'app richiede all'utente di impostare una password di complessità alta. Deve essere una password numerica (PIN) senza sequenze ripetute o ordinate oppure alfanumerica (password). Il PIN deve contenere almeno 8 cifre; la password deve contenere almeno 6 caratteri.

5. Se si desidera che l'utente abbia la possibilità di utilizzare le impronte digitali per sbloccare lo schermo, selezionare la casella di controllo **Consenti l'uso delle impronte digitali (per dispositivi con Android 9 o versioni precedenti)**. Se la password di sblocco non rispetta i requisiti di sicurezza aziendali, non è possibile utilizzare un lettore di impronte digitali per sbloccare lo schermo.

Nei dispositivi con Android 10.0 o versioni successive, l'uso dell'impronta digitale per sbloccare lo schermo non è supportato.

Kaspersky Endpoint Security for Android non limita l'utilizzo di un lettore di impronte digitali per l'accesso alle app o la conferma degli acquisti.

In determinati dispositivi Samsung, non è possibile impedire l'utilizzo delle impronte digitali per lo sblocco dello schermo.

In determinati dispositivi Samsung, se la password di sblocco non è conforme ai requisiti di sicurezza aziendali, Kaspersky Endpoint Security for Android non impedisce l'utilizzo delle impronte digitali per lo sblocco dello schermo.

Dopo aver aggiunto un'impronta digitale nelle impostazioni del dispositivo, l'utente può sbloccare lo schermo utilizzando i seguenti metodi:

- Posizionare il dito sul lettore di impronte digitali (metodo principale).
- Immettere la password di sblocco (metodo secondario).

6. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione della protezione dei dati di un dispositivo rubato o smarrito

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per proteggere i dati aziendali in caso di furto o smarrimento di un dispositivo mobile, è necessario configurare la protezione dall'accesso non autorizzato.

Per garantire la protezione dei dati del dispositivo rubato o smarrito, Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo.

Per configurare la protezione dei dati di un dispositivo rubato o smarrito:

1. Aprire la finestra delle proprietà dei criteri:
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.
2. Nella finestra delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Protezione essenziale**.
3. Nella sezione **Antifurto** configurare il blocco del dispositivo:
   - Specificare il numero di caratteri nel codice di sblocco.
   - Specificare il testo da visualizzare quando il dispositivo è bloccato.
4. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione del controllo app

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Controllo app verifica che le app installate in un dispositivo mobile siano conformi ai requisiti di sicurezza aziendali. In Kaspersky Security Center l'amministratore crea elenchi di app consentite, bloccate, obbligatorie e consigliate in base ai requisiti di sicurezza aziendali. In seguito a Controllo app, Kaspersky Endpoint Security richiede all'utente di installare le app obbligatorie e consigliate e di rimuovere le app bloccate. È impossibile avviare le app bloccate nel dispositivo mobile dell'utente.

In Kaspersky Security Center Web Console e Cloud Console è possibile gestire le app nei dispositivi degli utenti applicando regole predefinite. È possibile configurare due tipi di regole di **Controllo app**: regole dell'applicazione e regole della categoria.

Una **Regola dell'app** viene applicata a un'app specifica, mentre una **Regola della categoria** viene applicata a qualsiasi app appartenente a una categoria predefinita. Le categorie di app sono specificate dagli esperti di Kaspersky.

*Per configurare **Controllo app**:*

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Controlli di sicurezza**.

3. Nella tabella presente nella sezione **Controllo app** aggiungere le regole che definiranno quali app verranno controllate.

   - Per aggiungere una regola per un'app specifica:

     a. Nella tabella fare clic su **Regola dell'app**.

     b. Nella finestra **Regola dell'app** visualizzata scegliere l'azione che verrà eseguita con le app a cui si applica la regola creata.

     c. Specificare l'app che sarà soggetta alla regola compilando **Collegamento al pacchetto di installazione (ad esempio https://play.google.com/store/apps/details?id=com.kaspersky.kes)**, **Nome del pacchetto (ad esempio katana.facebook.com)** e **Nome app**.

     d. Fare clic su **Salva**.

     La regola viene aggiunta all'elenco delle regole di **Controllo app**.

   - Per aggiungere una regola per una categoria di app:

     a. Nella tabella nella sezione **Controllo app** fare clic su **Regola della categoria**.

     b. Nella finestra **Regola della categoria** visualizzata selezionare la categoria dell'app nell'elenco a discesa.

     Le app all'interno della categoria selezionata saranno soggette alla regola creata.

     c. Nella sezione **Modalità operativa** selezionare l'azione che verrà eseguita quando un'app all'interno della categoria selezionata tenterà di avviarsi: **App vietate** o **App consentite**.

     d. Se necessario, compilare il campo **Commento aggiuntivo mostrato nel dispositivo dell'utente quando viene rilevata un'app di una categoria specificata**.

     e. Fare clic su **Salva**.

     La regola viene aggiunta all'elenco delle regole di **Controllo app**.

4. Nella sezione **Azioni relative alle app vietate** scegliere quale azione viene eseguita per le applicazioni vietate:

   - Se si desidera che Kaspersky Endpoint Security for Android blocchi l'avvio di applicazioni vietate nel dispositivo mobile dell'utente, selezionare **Blocca l'avvio delle app**.
   - Se si desidera che Kaspersky Endpoint Security for Android invii dati sulle app vietate al registro eventi senza bloccarle, selezionare **Non bloccare le app vietate, segnala e basta**.

5. Nella sezione **Modalità operativa** scegliere se le regole aggiunte definiranno le app consentite o le app vietate:

   - Se si desidera che le regole definiscano quali app sono consentite, selezionare **App vietate**.

     Se si desidera che Kaspersky Endpoint Security for Android blocchi l'avvio delle app di sistema nel dispositivo mobile dell'utente (ad esempio Calendario, Fotocamera e Impostazioni) nella modalità **App vietate**, selezionare la casella **Blocca app di sistema**.

     > Gli esperti di Kaspersky consigliano di non bloccare le app di sistema poiché l'operazione potrebbe generare errori di funzionamento del dispositivo.

   - Se si desidera che le regole definiscano quali app sono vietate, selezionare **App consentite**.

6. Per ricevere informazioni su tutte le app installate nei dispositivi mobili, nella sezione **Rapporto sulle applicazioni** selezionare la casella **Invia un elenco delle app installate in tutti i dispositivi mobili**.

   Kaspersky Endpoint Security for Android invia i dati al registro eventi ogni volta che un'app viene installata o rimossa dal dispositivo.

7. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione del controllo conformità dei dispositivi mobili con i requisiti di sicurezza aziendali

> È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Il controllo conformità consente di monitorare i dispositivi Android per verificare la conformità con i requisiti di sicurezza aziendali e intraprendere azioni in caso di non conformità. I requisiti di sicurezza aziendali definiscono il modo in cui l'utente può utilizzare il dispositivo. Ad esempio, la protezione in tempo reale deve essere abilitata nel dispositivo, i database anti-virus devono essere aggiornati e la password del dispositivo deve essere sufficientemente complessa. Controllo conformità si basa su un elenco di regole. Una regola di conformità include i seguenti componenti:

- Criterio di non conformità del dispositivo.
- Azione che verrà eseguita in un dispositivo se l'utente non corregge la mancata conformità entro il periodo di tempo definito.
- Periodo di tempo assegnato all'utente per correggere la mancata conformità (ad esempio, 24 ore).

Al termine del periodo di tempo specificato, l'azione selezionata verrà eseguita nel dispositivo dell'utente.

In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

Per configurare il controllo conformità, è possibile eseguire le seguenti azioni:

- Abilitare o disabilitare le regole di conformità esistenti.
- Modificare una regola di conformità esistente.
- Aggiungere una nuova regola.
- Eliminare una regola.

Abilitazione e disabilitazione delle regole di conformità

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per abilitare o disabilitare le regole esistenti di controllo conformità dei dispositivi mobili con i requisiti di sicurezza aziendali:

1. Aprire la finestra delle proprietà dei criteri:
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.
2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Controlli di sicurezza**.
3. Nella sezione **Controllo conformità** abilitare o disabilitare le regole di conformità esistenti utilizzando gli interruttori nella colonna **Stato**.
4. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Modifica delle regole di conformità

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per modificare una regola per il controllo della conformità dei dispositivi mobili ai requisiti di sicurezza aziendali:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Controlli di sicurezza**.

3. Nella sezione **Controllo conformità** selezionare la regola che si desidera modificare, quindi fare clic su **Modifica**.

4. Nella finestra **Regola** visualizzata modificare la regola come segue:

   a. Nella colonna **Azione** configurare l'elenco delle azioni da eseguire in caso di non conformità alla regola aggiungendo nuove azioni, modificando le azioni esistenti o eliminandole.

   b. Facoltativamente, specificare il periodo di tempo in cui un utente può correggere la non conformità utilizzando la colonna **Tempo per la rettifica** per ogni azione.

   c. Fare clic sul pulsante **Salva** per salvare la regola.

5. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Aggiunta delle regole di conformità

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per aggiungere una regola per il controllo della conformità dei dispositivi mobili ai requisiti di sicurezza aziendali:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Controlli di sicurezza**.

3. Nella sezione **Controllo conformità** fare clic su **Regola**.

4. Nella finestra **Regola** visualizzata definire la regola come segue:

   a. Selezionare il criterio di non conformità per la regola.

   b. Fare clic su **Aggiungi**, quindi selezionare l' azione da eseguire in caso di non conformità con la regola nella colonna **Azione**.

   È possibile aggiungere diverse azioni.

   c. Specificare il periodo di tempo in cui un utente può correggere la non conformità utilizzando la colonna **Tempo per la rettifica** per ogni azione.

   d. Fare clic sul pulsante **Salva** per salvare la regola.

5. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Eliminazione delle regole di conformità

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per eliminare una regola per il controllo della conformità dei dispositivi mobili ai requisiti di sicurezza aziendali:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Controlli di sicurezza**.

3. Nella sezione **Controllo conformità** selezionare la regola che si desidera eliminare, quindi fare clic su **Elimina**.

4. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Elenco dei criteri di non conformità

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Per assicurarsi che un dispositivo Android sia conforme ai requisiti di sicurezza aziendali, Kaspersky Endpoint Security for Android può controllare il dispositivo in base ai seguenti criteri:

- **Protezione in tempo reale disabilitata**.

  La protezione in tempo reale deve essere abilitata.

  Per ulteriori informazioni sulla configurazione della protezione in tempo reale, vedere la sezione "Configurazione della protezione in tempo reale".

- **Database anti-virus non aggiornati**.

  Il database anti-virus di Kaspersky Endpoint Security for Android deve essere aggiornato regolarmente.

  Per ulteriori informazioni sulla definizione delle impostazioni degli aggiornamenti dei database anti-virus, vedere la sezione "Configurazione della protezione anti-virus".

- **App vietate installate**.

  Nel dispositivo non devono essere installate applicazioni classificate come **Blocca l'avvio**, come specificato nella sezione **Controllo app**.

  Per ulteriori informazioni sulla creazione di regole per le applicazioni, vedere la sezione " Configurazione del controllo app".

- **Installate app appartenenti alle categorie vietate**.

  Nel dispositivo non devono essere installate applicazioni che rientrano in una categoria classificata come **Blocca l'avvio**, come specificato nella sezione **Controllo app**.

  Per ulteriori informazioni sulla creazione di regole per le categorie di applicazioni, vedere la sezione " Configurazione del controllo app".

- **Non tutte le app obbligatorie sono installate**.

  Nel dispositivo devono essere installate applicazioni specifiche classificate come **Forza installazione**, come specificato nella sezione **Controllo app**.

  Per ulteriori informazioni sulla creazione di regole per le applicazioni, vedere la sezione " Configurazione del controllo app".

- **Versione del sistema operativo non aggiornata**.

  Il dispositivo deve disporre di una versione consentita del sistema operativo.

  Per utilizzare questo criterio di non conformità, è necessario specificare l'intervallo di versioni del sistema operativo consentite negli elenchi a discesa **Versione minima del sistema operativo** e **Versione massima del sistema operativo**.

- **Il dispositivo non viene sincronizzato da molto tempo**.

  Il dispositivo deve essere regolarmente sincronizzato con Administration Server.

  Per utilizzare questo criterio di non conformità, è necessario specificare l'intervallo di tempo massimo tra le sincronizzazioni del dispositivo nell'elenco a discesa **Periodo di sincronizzazione**.

- **Il dispositivo è stato dotato dell'accesso root**.

  Il dispositivo non deve essere dotato dell'accesso root.

  Per ulteriori informazioni, vedere la sezione "Rilevamento delle manomissioni dei dispositivi Android (root)".

- **La password di sblocco non è conforme ai requisiti di sicurezza**.

Il dispositivo deve essere protetto con una password di sblocco conforme ai requisiti di complessità della password di sblocco.

Elenco delle azioni in caso di non conformità

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Se l'utente non risolve un problema di non conformità entro il periodo di tempo specificato, sono disponibili le seguenti azioni:

- **Blocca tutte le app tranne le app di sistema**.

  L'avvio di tutte le app nel dispositivo mobile dell'utente, ad eccezione di quelle di sistema, è bloccato.

- **Blocca dispositivo**.

  Il dispositivo mobile è bloccato. Per ottenere l'accesso ai dati, è necessario sbloccare il dispositivo. Se il motivo del blocco del dispositivo non viene rettificato dopo lo sblocco del dispositivo, il dispositivo verrà bloccato nuovamente dopo il periodo di tempo specificato.

- **Cancella dati aziendali**.

  Cancellare i dati inseriti nei contenitori, l'account e-mail aziendale, le impostazioni per la connessione alla rete Wi-Fi aziendale e alla VPN e l'APN (Access Point Name).

- **Ripristina tutte le impostazioni predefinite del dispositivo**.

  Tutti i dati vengono eliminati dal dispositivo mobile e viene eseguito il rollback delle impostazioni ai valori predefiniti.

Configurazione dell'accesso dell'utente ai siti Web

È possibile definire queste impostazioni dei criteri per i dispositivi Android e iOS.

Per proteggere i dati personali e aziendali archiviati nei dispositivi mobili durante la navigazione in Internet, è possibile configurare l'accesso degli utenti ai siti Web utilizzando Protezione Web. Protezione Web esegue la scansione dei siti Web prima che un utente li apra, quindi blocca i siti Web che distribuiscono codice dannoso e i siti Web di phishing progettati per rubare dati riservati e ottenere l'accesso ai conti finanziari.

Per i dispositivi Android questa funzionalità supporta anche il filtro dei siti Web in base alle categorie definite nel servizio cloud Kaspersky Security Network. Il filtro consente di limitare l'accesso a determinati siti Web o categorie di siti Web (ad esempio, quelli delle categorie "**Gioco d'azzardo, lotterie, concorsi a premi**" o "**Comunicazioni di rete**").

Nei dispositivi Android Protezione Web funziona solo nel browser Google Chrome, in Huawei Browser e Samsung Internet Browser.

Per garantire il corretto funzionamento di Protezione Web, Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo.

Nei dispositivi iOS l'utente deve consentire l'app Kaspersky Security for iOS per aggiungere una configurazione VPN e garantire il funzionamento di Protezione Web.

Per configurare l'accesso dell'utente ai siti Web:

1. Aprire la finestra delle proprietà dei criteri:
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.
2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Controlli di sicurezza**.
3. Nella sezione **Protezione Web** selezionare la casella di controllo **Abilita Protezione Web** per abilitare la funzionalità.
4. Per i dispositivi Android è possibile selezionare una delle seguenti opzioni:
   - Per limitare l'accesso degli utenti ai siti Web in base al contenuto:
     a. Selezionare **Blocca i siti Web di determinate categorie**.
     b. Selezionare le caselle di controllo accanto alle categorie di siti Web a cui Kaspersky Endpoint Security for Android bloccherà l'accesso.

     Se Protezione Web è abilitato, l'accesso dell'utente ai siti Web nelle categorie **Phishing** e **Siti malware** è sempre bloccato.
   - Per specificare l'elenco dei siti Web consentiti:
     a. Selezionare **Consenti solo i siti Web specificati**.
     b. Creare un elenco di siti Web aggiungendo gli indirizzi dei siti Web ai quali l'app non bloccherà l'accesso. Kaspersky Endpoint Security for Android supporta solo espressioni regolari. Durante l'immissione dell'indirizzo di un sito Web consentito, utilizzare i seguenti modelli:
        - `http:\/\/www\.example\.com.*`: tutte le pagine secondarie dei siti Web sono consentite (ad esempio `http://www.example.com/about`).
        - `https:\/\/.*example\.com`: tutte le pagine del sottodominio del sito Web sono consentite (ad esempio `https://pictures.example.com`).

c. È inoltre possibile utilizzare l'espressione `https?` per selezionare HTTP e HTTPS. Per maggiori informazioni sulle espressioni regolari, fare riferimento al sito Web dell'assistenza tecnica di Oracle.

- Per bloccare l'accesso degli utenti a tutti i siti Web, selezionare **Blocca tutti i siti Web**.

5. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione delle restrizioni per le funzionalità

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Kaspersky Security Center Web Console consente di configurare l'accesso degli utenti alle seguenti funzionalità dei dispositivi mobili:

- Wi-Fi
- Fotocamera
- Bluetooth

Per impostazione predefinita, l'utente può utilizzare il Wi-Fi, la fotocamera e il Bluetooth nel dispositivo senza restrizioni.

Per configurare le restrizioni di utilizzo del Wi-Fi, della fotocamera e del Bluetooth nel dispositivo:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Controlli di sicurezza**.

3. Nella sezione **Gestione funzionalità** configurare l'utilizzo del Wi-Fi, della fotocamera e della connettività Bluetooth:

   - Per disabilitare il modulo Wi-Fi nel dispositivo mobile dell'utente, selezionare la casella **Impedisci l'uso del Wi-Fi**.

     Nei dispositivi con Android 10.0 o versioni successive, il divieto di utilizzo delle reti Wi-Fi non è supportato.

- Per disabilitare la fotocamera nel dispositivo mobile dell'utente, selezionare la casella **Impedisci l'uso della fotocamera**.

  Nei dispositivi che eseguono Android 10.0 o versioni successive, l'utilizzo della fotocamera non può essere completamente vietato.

  Nei dispositivi che eseguono Android 11 o versioni successive Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo. In tal caso, non sarà possibile limitare l'utilizzo della fotocamera.

- Per disabilitare la connettività Bluetooth nel dispositivo mobile dell'utente, selezionare la casella **Impedisci l'uso del Bluetooth**.

  In Android 12 o versioni successive l'utilizzo del Bluetooth può essere disabilitato solo se l'utente del dispositivo ha concesso l'autorizzazione **Dispositivi Bluetooth nelle vicinanze**. L'utente può concedere questa autorizzazione durante la procedura guidata di configurazione iniziale o in un secondo momento.

4. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Protezione di Kaspersky Endpoint Security for Android dalla rimozione

Per la protezione dei dispositivi mobili e la conformità con i requisiti di sicurezza aziendali, è possibile abilitare la protezione dalla rimozione di Kaspersky Endpoint Security for Android. In questo caso, l'utente non può rimuovere l'app utilizzando l'interfaccia di Kaspersky Endpoint Security for Android. Durante la rimozione dell'app tramite gli strumenti del sistema operativo Android, all'utente viene richiesto di disabilitare i diritti di amministratore per Kaspersky Endpoint Security for Android. Dopo aver disabilitato i diritti, il dispositivo mobile verrà bloccato.

Per abilitare la protezione dalla rimozione di Kaspersky Endpoint Security for Android:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Controlli di sicurezza**.

3. Nella sezione **Gestisci app nel dispositivo mobile** deselezionare la casella di controllo **Consenti la rimozione di Kaspersky Endpoint Security for Android dal dispositivo**.

Per proteggere l'app dalla rimozione nei dispositivi che eseguono Android 7.0 o versioni successive, Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Durante l'esecuzione della procedura guidata di configurazione iniziale, Kaspersky Endpoint Security for Android richiede all'utente di concedere all'applicazione tutte le autorizzazioni richieste. L'utente può ignorare questi passaggi o disabilitare tali autorizzazioni nelle impostazioni del dispositivo in un momento successivo. In tal caso, l'app non è protetta dalla rimozione.

4. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Se viene effettuato un tentativo di rimozione dell'app, il dispositivo mobile verrà bloccato.

Configurazione della sincronizzazione dei dispositivi mobili con Kaspersky Security Center

È possibile definire queste impostazioni dei criteri per i dispositivi Android e iOS.

Per gestire i dispositivi mobili e ricevere rapporti o statistiche dai dispositivi mobili, è necessario definire le impostazioni di sincronizzazione. La sincronizzazione dei dispositivi mobili con Kaspersky Security Center può essere eseguita nei seguenti modi:

- **In base alla pianificazione**. La sincronizzazione in base alla pianificazione viene eseguita tramite HTTP. È possibile configurare la pianificazione della sincronizzazione nelle proprietà dei criteri. Le modifiche apportate alle impostazioni dei criteri, a comandi e attività verranno eseguite durante la sincronizzazione dei dispositivi mobili con Kaspersky Security Center in base alla pianificazione, e quindi con un ritardo. Per impostazione predefinita, i dispositivi mobili vengono sincronizzati automaticamente con Kaspersky Security Center ogni sei ore.

  In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

- **Forzata** (per i dispositivi Android). La sincronizzazione forzata viene eseguita utilizzando le notifiche push del servizio FCM (Firebase Cloud Messaging). La sincronizzazione forzata è orientata principalmente all'invio tempestivo dei comandi a un dispositivo mobile. Se si desidera utilizzare la sincronizzazione forzata, assicurarsi che le impostazioni FCM siano configurate in Kaspersky Security Center.

Per configurare la sincronizzazione dei dispositivi mobili con Kaspersky Security Center:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Sincronizzazione**.

3. Nella sezione **Sincronizzazione con Administration Server** utilizzare l'elenco a discesa **Periodo di sincronizzazione** per selezionare il periodo di sincronizzazione.

   Per impostazione predefinita, la sincronizzazione viene eseguita ogni sei ore.

4. Per i dispositivi Android è possibile disabilitare la sincronizzazione quando il dispositivo è in roaming. A tale scopo, selezionare la casella di controllo **Non sincronizzare in roaming**.

   Per impostazione predefinita, la sincronizzazione in roaming è abilitata.

5. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Kaspersky Security Network

Per proteggere i dispositivi mobili più efficacemente, Kaspersky Endpoint Security for Android e Kaspersky Security for iOS utilizzano dati acquisiti da utenti di tutto il mondo. L'elaborazione di questi dati viene eseguita tramite *Kaspersky Security Network*.

Kaspersky Security Network (KSN) è un'infrastruttura di servizi cloud che consente l'accesso alla Knowledge Base online di Kaspersky con informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce una risposta più rapida da parte delle applicazioni Kaspersky alle nuove minacce, migliora le prestazioni di alcuni componenti di protezione e riduce la probabilità di falsi allarmi.

La partecipazione a Kaspersky Security Network consente a Kaspersky di acquisire informazioni in tempo reale sui tipi e sulle origini delle nuove minacce, sviluppare metodi per la loro neutralizzazione e ridurre il numero di falsi allarmi. La partecipazione a Kaspersky Security Network consente inoltre di accedere alle statistiche sulla reputazione di applicazioni e siti Web.

Quando si partecipa a Kaspersky Security Network, alcune statistiche vengono acquisite durante l'esecuzione dell'app mobile e vengono inviate automaticamente a Kaspersky. Queste informazioni rendono possibile tenere traccia delle minacce in tempo reale. I file o le relative parti che possono essere sfruttati da utenti malintenzionati per danneggiare il computer o i contenuti dell'utente possono anche essere inviati a Kaspersky per un'ulteriore analisi.

I seguenti componenti dell'app utilizzano il servizio cloud Kaspersky Security Network:

- I componenti Anti-Virus, Protezione Web e Controllo app nell'app Kaspersky Endpoint Security for Android.
- Il componente Protezione Web nell'app Kaspersky Security for iOS.

Per iniziare a utilizzare KSN, è necessario accettare i termini e le condizioni del Contratto di licenza con l'utente finale. Per ulteriori informazioni sull'invio dei dati a KSN, fare riferimento allo scambio di informazioni con Kaspersky Security Network.

Il rifiuto di partecipare a KSN comporta la riduzione del livello di protezione del dispositivo, che può provocare l'infezione del dispositivo e la perdita dei dati.

Per migliorare le prestazioni dell'app mobile, è inoltre possibile fornire dati statistici aggiuntivi a Kaspersky Security Network.

L'invio delle informazioni a Kaspersky Security Network è volontario.

Scambio di informazioni con Kaspersky Security Network

Scambio di informazioni in Kaspersky Endpoint Security for Android

Per migliorare la protezione in tempo reale, Kaspersky Endpoint Security for Android utilizza il servizio cloud Kaspersky Security Network per l'esecuzione dei seguenti componenti:

- **Anti-Virus.** L'app ottiene accesso alla Knowledge Base online di Kaspersky, con informazioni sulla reputazione di file e app. La scansione viene eseguita per le minacce per cui non sono state ancora aggiunte informazioni ai database anti-virus, ma che sono già disponibili in KSN. Il servizio cloud di Kaspersky Security Network garantisce l'esecuzione completa di Anti-virus e riduce la probabilità di falsi allarmi.

- **Protezione Web.** L'app utilizza i dati ricevuti da KSN per esaminare i siti Web prima dell'apertura. L'app determina inoltre la categoria del sito Web per controllare l'accesso a Internet degli utenti in base agli elenchi delle categorie consentite e bloccate (ad esempio, la categoria "Comunicazioni di rete").

- **Controllo app.** L'app determina la categoria dell'app per limitare l'avvio delle app che non soddisfano i requisiti di sicurezza aziendali in base agli elenchi delle categorie consentite e bloccate (ad esempio, la categoria "Giochi").

Le informazioni sul tipo di dati inviati a Kaspersky durante l'utilizzo di KSN con Anti-Virus e Controllo app sono disponibili nel Contratto di licenza con l'utente finale. Accettando i termini e le condizioni del Contratto di licenza, si accetta il trasferimento di queste informazioni.

Le informazioni sul tipo di dati inviati a Kaspersky durante l'utilizzo di KSN con Protezione Web sono disponibili nell'Informativa relativa all'elaborazione dei dati per Protezione Web. Accettando i termini e le condizioni dell'Informativa, si accetta il trasferimento di queste informazioni.

Per ulteriori informazioni sulla trasmissione dei dati a KSN, fare riferimento alla sezione Trasmissione dei dati in Kaspersky Endpoint Security for Android.

La trasmissione dei dati a KSN è volontaria. Se lo si desidera, è possibile disabilitare lo scambio dei dati con KSN.

Scambio di informazioni in Kaspersky Security for iOS

Per migliorare la protezione in tempo reale, Kaspersky Security for iOS utilizza il servizio cloud Kaspersky Security Network per l'esecuzione del componente **Protezione Web**. L'app utilizza i dati ricevuti da KSN per esaminare le risorse Web prima dell'apertura.

Le informazioni sul tipo di dati inviati a Kaspersky durante l'utilizzo di KSN con Protezione Web sono disponibili nel Contratto di licenza con l'utente finale. Accettando i termini e le condizioni del Contratto di licenza, si accetta il trasferimento di queste informazioni.

Per ulteriori informazioni sulla trasmissione dei dati a KSN, fare riferimento alla sezione Trasmissione dei dati in Kaspersky Security for iOS.

La trasmissione dei dati a KSN è volontaria. Se lo si desidera, è possibile disabilitare lo scambio dei dati con KSN.

Invio delle statistiche a KSN dalle app Android e iOS

Per consentire lo scambio dei dati con KSN al fine di migliorare le prestazioni dell'app, devono essere soddisfatte le seguenti condizioni:

- L'utente del dispositivo deve leggere e accettare i termini dell'Informativa di Kaspersky Security Network.
- È necessario configurare le impostazioni del criterio di gruppo per consentire l'invio delle statistiche a KSN.

È possibile scegliere di interrompere l'invio di dati statistici a Kaspersky Security Network in qualsiasi momento. Le informazioni sul tipo di dati statistici inviati a Kaspersky durante l'utilizzo di KSN con l'app mobile sono disponibili nell'Informativa di Kaspersky Security Network.

Abilitazione e disabilitazione di Kaspersky Security Network

Per impostazione predefinita, l'utilizzo di Kaspersky Security Network è abilitato.

Se l'utilizzo di Kaspersky Security Network è disabilitato, Protezione Web, Controllo app e la protezione aggiuntiva in Kaspersky Security Network vengono disabilitati automaticamente e le relative impostazioni diventano non disponibili.

Per abilitare o disabilitare l'utilizzo di Kaspersky Security Network:

1. Aprire la finestra delle proprietà dei criteri:
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.
   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.
2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **KSN e statistiche**.
3. Per abilitare o disabilitare l'utilizzo di Kaspersky Security Network, selezionare o deselezionare la casella di controllo **Usa Kaspersky Security Network**.
4. Se l'utilizzo di Kaspersky Security Network è abilitato e si accetta di inviare i dati a Kaspersky, selezionare la casella di controllo **Consenti l'invio delle statistiche a Kaspersky Security Network**. L'utilizzo di questi dati garantisce una risposta più rapida alle nuove minacce da parte dell'app mobile, migliora le prestazioni dei componenti di protezione e riduce la probabilità di falsi allarmi.
5. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Scambio di informazioni con Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Kaspersky Endpoint Security for Android scambia dati con i servizi Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics al fine di migliorare la qualità, l'aspetto e le prestazioni del software, dei prodotti, dei servizi e dell'infrastruttura Kaspersky analizzando l'esperienza degli utenti, le funzionalità, lo stato e le impostazioni del dispositivo in uso.

Lo scambio di informazioni con i servizi Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics è disabilitato per impostazione predefinita.

Per abilitare lo scambio dei dati:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **KSN e statistiche**.

3. Nella sezione **Invio delle statistiche** selezionare la casella di controllo **Consenti il trasferimento dei dati per migliorare la qualità, l'aspetto e le prestazioni dell'app**.

4. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

   Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione delle notifiche nei dispositivi mobili

È possibile definire queste impostazioni dei criteri solo per i dispositivi Android.

Se si desidera che l'utente del dispositivo mobile non venga distratto dalle notifiche di Kaspersky Endpoint Security for Android, è possibile disabilitare determinate notifiche.

Kaspersky Endpoint Security utilizza i seguenti strumenti per visualizzare lo stato della protezione del dispositivo:

- **Notifica relativa allo stato della protezione**. Questa notifica viene visualizzata nella barra delle notifiche. Una notifica relativa allo stato della protezione non può essere rimossa. La notifica visualizza lo stato della protezione del dispositivo (ad esempio) e il numero di problemi, se presenti. L'utente del dispositivo può toccare lo stato della protezione del dispositivo e visualizzare i problemi elencati nell'app.

- **Notifiche dell'app**. Queste notifiche danno informazioni sull'applicazione all'utente del dispositivo (ad esempio sul rilevamento delle minacce).

- **Messaggi pop-up**. I messaggi pop-up richiedono l'intervento dell'utente del dispositivo (ad esempio quando viene rilevata una minaccia).

Tutte le notifiche di Kaspersky Endpoint Security for Android sono abilitate per impostazione predefinita.

L'utente di un dispositivo Android può disabilitare tutte le notifiche di Kaspersky Endpoint Security for Android nelle impostazioni nella barra di notifica. Se le notifiche sono disabilitate, l'utente non monitora l'esecuzione dell'app e potrebbe ignorare informazioni importanti (ad esempio, le informazioni sugli errori durante la sincronizzazione del dispositivo con Kaspersky Security Center). In questo caso, per visualizzare lo stato dell'app, l'utente deve aprire Kaspersky Endpoint Security for Android.

Per configurare la visualizzazione delle notifiche sull'esecuzione di Kaspersky Endpoint Security for Android in un dispositivo mobile:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Notifiche e rapporti**.

3. Nella sezione **Notifiche** configurare la visualizzazione delle notifiche:

   - Per nascondere tutte le notifiche e i messaggi pop-up, disabilitare l'interruttore **Visualizza le notifiche quando Kaspersky Endpoint Security è in background**.

     Kaspersky Endpoint Security for Android visualizzerà solo la notifica sullo stato della protezione. La notifica visualizza lo stato della protezione del dispositivo (ad esempio) e il numero di problemi. L'app visualizza le notifiche anche quando l'utente utilizza l'app (ad esempio l'utente aggiorna manualmente i database anti-virus).

     Gli esperti di Kaspersky consigliano di abilitare le notifiche e i messaggi pop-up. Se si disabilitano le notifiche e i messaggi pop-up quando l'app è in background, l'app non avviserà gli utenti delle minacce in tempo reale. Gli utenti dei dispositivi mobili possono scoprire lo stato della protezione del dispositivo solo quando aprono l'app.

   - In **Elenco dei problemi di sicurezza visualizzato nei dispositivi degli utenti** selezionare i problemi di Kaspersky Endpoint Security for Android che si desidera visualizzare nel dispositivo mobile dell'utente.

4. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Rilevamento delle manomissioni dei dispositivi

Kaspersky Security Center Web Console consente di rilevare manomissioni dei dispositivi (root) nei dispositivi Android e jailbreak nei dispositivi iOS. In un dispositivo manomesso i file di sistema non sono protetti e quindi possono essere modificati. Inoltre, nei dispositivi manomessi possono essere installate app di terze parti da origini sconosciute. Al rilevamento di un tentativo di manomissione, è consigliabile ripristinare immediatamente il normale funzionamento del dispositivo.

Kaspersky Endpoint Security for Android utilizza i seguenti servizi per rilevare quando un utente ottiene i privilegi di root:

- *Servizio integrato di Kaspersky Endpoint Security for Android.* Un servizio Kaspersky che verifica se l'utente di un dispositivo mobile ha ottenuto i privilegi di root (Kaspersky Mobile Security SDK).

- *Attestazione SafetyNet.* Un servizio di Google che controlla l'integrità del sistema operativo, analizza l'hardware e il software del dispositivo e identifica altri problemi di sicurezza. Per maggiori informazioni sull'attestazione SafetyNet, visitare il sito Web dell'assistenza tecnica di Android.

Kaspersky Security for iOS utilizza il seguente servizio per rilevare un jailbreak:

- *Servizio integrato di Kaspersky Security for iOS.* Un servizio Kaspersky che verifica se un dispositivo mobile è stato sottoposto a jailbreak (Kaspersky Mobile Security SDK).

Se un dispositivo è risulta manomesso, l'utente riceve una notifica. È possibile visualizzare le notifiche sulle manomissioni in Kaspersky Security Center Web Console nella scheda **MONITORAGGIO E GENERAZIONE DEI RAPPORTI** > **DASHBOARD.** È inoltre possibile disabilitare le notifiche delle manomissioni nelle impostazioni di notifica degli eventi.

Nei dispositivi Android è possibile imporre restrizioni sull'attività dell'utente se il dispositivo risulta manomesso (ad esempio, il blocco del dispositivo). È possibile imporre restrizioni utilizzando il componente Controllo conformità. A tale scopo, creare una regola di conformità con il criterio **Il dispositivo è stato dotato dell'accesso root**.

Definizione delle impostazioni di licenza

È possibile definire queste impostazioni dei criteri per i dispositivi Android e iOS.

Per gestire i dispositivi mobili in Kaspersky Security Center Web Console o Cloud Console, è necessario attivare l'app mobile nei dispositivi mobili. L'attivazione dell'app Kaspersky Endpoint Security for Android o dell'app Kaspersky Security for iOS in un dispositivo mobile viene eseguita fornendo all'app informazioni di licenza valide. Le informazioni sulla licenza vengono distribuite al dispositivo mobile insieme al criterio quando il dispositivo viene sincronizzato con Kaspersky Security Center.

Se l'attivazione dell'app mobile non viene completata entro 30 giorni dal momento dell'installazione nel dispositivo mobile, l'app passerà automaticamente alla modalità con funzionalità limitate. In questa modalità, la maggior parte dei componenti dell'app non è operativa. Quando passa alla modalità con funzionalità limitate, l'app smette di eseguire la sincronizzazione automatica con Kaspersky Security Center. Pertanto, se l'attivazione dell'app non viene completata entro 30 giorni dall'installazione, l'utente deve sincronizzare manualmente il dispositivo con Kaspersky Security Center.

Per definire le impostazioni di licenza di un criterio di gruppo:

1. Aprire la finestra delle proprietà dei criteri:

   - Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **CRITERI E PROFILI**. Nell'elenco dei criteri di gruppo visualizzato fare clic sul nome del criterio che si desidera configurare.

- Nella finestra principale di Kaspersky Security Center Web Console o Cloud Console selezionare **DISPOSITIVI** > **MOBILE** > **DISPOSITIVI**. Fare clic sul dispositivo mobile che rientra nel criterio che si desidera configurare, quindi selezionare il criterio nella scheda **CRITERI ATTIVI E PROFILI CRITERIO**.

2. Nella pagina delle proprietà dei criteri selezionare **IMPOSTAZIONI APPLICAZIONE** > **Licenze**.

3. Utilizzare l'elenco a discesa per selezionare la chiave di licenza desiderata dall'archivio delle chiavi di Administration Server.

   I dettagli della chiave di licenza sono visualizzati nei campi di seguito.

   È possibile sostituire la chiave di attivazione esistente nel dispositivo mobile se è diversa da quella selezionata nell'elenco a discesa precedente. A tale scopo, selezionare la casella di controllo **Se la chiave nel dispositivo è diversa, sostituisci con questa chiave**.

4. Fare clic sul pulsante **Salva** per salvare le modifiche apportate al criterio e chiudere la finestra delle proprietà del criterio.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione degli eventi

È possibile definire queste impostazioni dei criteri per i dispositivi Android e iOS.

È possibile definire le impostazioni di archiviazione e notifica degli eventi che si verificano nei dispositivi degli utenti e che vengono inviati a Kaspersky Security Center.

È possibile configurare gli eventi solo quando si modifica un criterio.

Gli eventi vengono distribuiti per livello di importanza nelle seguenti schede:

- **Critico**

  Un evento critico indica un problema che può causare la perdita di dati, un malfunzionamento operativo o un errore critico.

- **Errore funzionale**

  Un errore funzionale indica un problema grave, un errore o un malfunzionamento che si è verificato durante il funzionamento dell'app.

- **Avviso**

  Un avviso non è necessariamente grave, ma indica comunque un potenziale problema futuro.

- **Informazioni**

  Un evento informativo notifica il completamento di un'operazione o di una procedura oppure il corretto funzionamento dell'app.

In ogni sezione l'elenco mostra i tipi di eventi e il periodo di archiviazione degli eventi predefinito in Kaspersky Security Center (in giorni).

Nell'elenco degli eventi è possibile effettuare le seguenti operazioni:

- Aggiungere o rimuovere un tipo di evento dall'elenco dei tipi di eventi inviati a Kaspersky Security Center.
- Definire le impostazioni di archiviazione e notifica per ogni tipo di evento, ad esempio: per quanto tempo gli eventi di questo tipo devono essere archiviati nel database di Administration Server o se si riceverà una notifica in merito agli eventi di questo tipo tramite e-mail.

Per ulteriori dettagli sulla configurazione degli eventi in Kaspersky Security Center Web Console e Cloud Console:

- Se si utilizza Kaspersky Security Center Web Console, fare riferimento alla *Guida di Kaspersky Security Center*.
- Se si utilizza Kaspersky Security Center Cloud Console, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

Configurazione degli eventi relativi all'installazione, all'aggiornamento e alla rimozione delle app nei dispositivi degli utenti

È possibile definire queste impostazioni dei criteri per i dispositivi Android e iOS.

Se si utilizza Kaspersky Security Center Cloud Console, l'elenco dei tipi di eventi che si verificano nei dispositivi degli utenti e vengono inviati a Kaspersky Security Center non include l'installazione, l'aggiornamento e la rimozione delle app nei dispositivi. Ciò è dovuto al fatto che tali eventi si verificano spesso e possono sostituire altri eventi importanti nel database di Kaspersky Security Center quando viene raggiunto il numero di eventi limite. Possono inoltre influire sulle prestazioni di Administration Server o del DBMS e sulla larghezza di banda della connessione Internet con Kaspersky Security Center Cloud Console.

Se si desidera comunque archiviare gli eventi di questo tipo e ricevere le relative notifiche, procedere come descritto in questa sezione.

Per configurare gli eventi relativi all'installazione, all'aggiornamento e alla rimozione delle app nei dispositivi degli utenti:

1. Nelle impostazioni di un criterio, nella scheda **CONFIGURAZIONE EVENTI**, aggiungere il tipo di evento informativo **App installata o rimossa (elenco delle app installate)** all'elenco degli eventi archiviati nel database di Administration Server.

   Per ulteriori dettagli sulla configurazione degli eventi, fare riferimento alla *Guida di Kaspersky Security Center Cloud Console*.

2. Abilitare l'opzione **Invia un elenco delle app installate in tutti i dispositivi mobili**.

Gli eventi relativi all'installazione, all'aggiornamento e alla rimozione delle app nei dispositivi degli utenti vengono archiviati nel database di Kaspersky Security Center. Si riceverà una notifica in merito a questi eventi.

Carico di rete

Questa sezione contiene informazioni sul volume del traffico di rete scambiato tra i dispositivi mobili e Kaspersky Security Center.

Volume del traffico

Attività	Traffico in uscita	Traffico in entrata	Traffico totale
Distribuzione iniziale dell'app, MB	0,08	17,76	17,84
Aggiornamento iniziale dei database anti-virus (il volume di traffico può variare a seconda delle dimensioni dei database anti-virus), MB	0,04	2,21	2,25
Sincronizzazione del dispositivo mobile con Kaspersky Security Center, MB	0,03	0,02	0,05
Aggiornamento periodico dei database anti-virus (il volume di traffico può variare a seconda delle dimensioni dei database anti-virus), MB	0,08	3,06	3,14
Esecuzione dei comandi di Antifurto. Localizza dispositivo (il volume di traffico può variare a seconda delle specifiche della fotocamera incorporata e della qualità delle immagini), MB	0,09	0,8	0,17
Esecuzione dei comandi di Antifurto. Foto utente, MB	1,0	0,02	1,02
Esecuzione dei comandi di Antifurto. Blocco Dispositivo, MB	0,06	0,05	0,11
Volume giornaliero medio, MB	0,22	6,96	7,18

Utilizzo di Administration Console basata su MMC

Questa sezione della Guida descrive la protezione e la gestione dei dispositivi mobili tramite Administration Console basata su MMC di Kaspersky Security Center.

Casi di utilizzo principali

INSTALLAZIONE

Come è possibile installare in remoto Kaspersky Endpoint Security for Android?

Come è possibile impedire a un utente di rimuovere Kaspersky Endpoint Security for Android?

Come è possibile attivare Kaspersky Endpoint Security for Android?

PROTEZIONE

Come è possibile bloccare un dispositivo smarrito o rubato?

Come è possibile proteggersi dalle minacce Internet?

Come è possibile vietare l'utilizzo di una password vuota?

UTILIZZO DI SOLUZIONI DI TERZE PARTI

Android Enterprise (Applicazioni con icona a forma di valigia, Configurazione del profilo lavoro Android)

VMware AirWatch, MobileIron, IBM Maas360, SOTI MobiControl

CONTROLLO

Come è possibile impedire a un utente di giocare in un dispositivo?

Come è possibile configurare l'accesso ai siti Web in un dispositivo?

Come è possibile rilevare root?

GESTIONE

Come è possibile configurare una cassetta postale in un dispositivo?

Come è possibile connettere un dispositivo mobile al Wi-Fi?

Come è possibile installare un'app aziendale?

Informazioni su Kaspersky Security for Mobile

Kaspersky Security for Mobile è una soluzione integrata per la protezione e la gestione dei dispositivi mobili aziendali, nonché dei dispositivi mobili personali utilizzati dai dipendenti dell'azienda per scopi aziendali.

Kaspersky Security for Mobile include i seguenti componenti:

- App mobile Kaspersky Endpoint Security for Android

  L'app Kaspersky Endpoint Security for Android garantisce la protezione dei dispositivi mobili da minacce Web, virus e altri programmi che rappresentano minacce.

- Plug-in di amministrazione di Kaspersky Endpoint Security for Android.

Il plug-in di amministrazione di Kaspersky Endpoint Security for Android fornisce l'interfaccia per la gestione dei dispositivi mobili e delle app mobili installate in essi tramite Administration Console di Kaspersky Security Center.

- Plug-in di amministrazione di Kaspersky Device Management for iOS

  Il Plug-in di Amministrazione di Kaspersky Device Management for iOS consente di definire le impostazioni di configurazione per i dispositivi connessi a Kaspersky Security Center tramite il protocollo MDM iOS (di seguito denominati "Dispositivi MDM iOS") e il protocollo Exchange ActiveSync (di seguito denominati "Dispositivi EAS"), senza utilizzare l'utilità di configurazione iPhone o la console di gestione di Exchange.

I plug-in di amministrazione sono integrati nel *sistema di amministrazione remota Kaspersky Security Center*. L'amministratore può utilizzare una singola Administration Console di Kaspersky Security Center per gestire tutti i dispositivi mobili nella rete aziendale, nonché i computer client e i sistemi virtuali. In seguito alla connessione all'Administration Server, i dispositivi mobili diventano gestiti. L'amministratore può monitorare in remoto i dispositivi gestiti.

L'app mobile Kaspersky Endpoint Security for Android può funzionare anche nell'ambito del *sistema di amministrazione remota di Kaspersky Endpoint Security Cloud*. Per maggiori informazioni sull'utilizzo delle app tramite Kaspersky Endpoint Security Cloud, fare riferimento alla *guida online di Kaspersky Endpoint Security Cloud*.

L'app mobile Kaspersky Endpoint Security for Android può anche funzionare nell'ambito delle soluzioni EMM di terze parti dei partecipanti alla community AppConfig.

Funzionalità chiave per la gestione dei dispositivi mobili in Administration Console basata su MMC

Kaspersky Security for Mobile offre le seguenti funzionalità:

- Distribuzione di messaggi e-mail per la connessione dei dispositivi Android a Kaspersky Security Center tramite i collegamenti a Google Play.
- Connessione remota dei dispositivi mobili a Kaspersky Security Center e altri sistemi EMM di terze parti (ad esempio VMWare AirWatch, MobileIron, IBM Maas360, SOTI MobiControl).
- Configurazione remota dell'app Kaspersky Endpoint Security for Android e configurazione remota di servizi, app e funzioni dei dispositivi Android.
- Configurazione remota dei dispositivi mobili in base ai requisiti di sicurezza aziendale.
- Impedimento della fuga di informazioni aziendali memorizzate nei dispositivi mobili, in caso di furto o smarrimento (Antifurto).
- Controllo della conformità ai requisiti di sicurezza aziendali (Controllo conformità).
- Controllo dell'utilizzo di Internet nei dispositivi mobili (Protezione Web).
- Installazione della posta elettronica aziendale nei dispositivi mobili, incluse le organizzazioni con un server e-mail Microsoft Exchange distribuito nell'azienda (solo per dispositivi Samsung e iOS).
- Configurazione della rete aziendale (Wi-Fi, VPN) per l'utilizzo della VPN nei dispositivi mobili. La VPN può essere configurata solo nei dispositivi Samsung e iOS.

- Configurazione della visualizzazione dello stato del dispositivo mobile in Kaspersky Security Center in caso di violazione delle regole dei criteri: Critico, Avviso, OK.
- Configurazione delle notifiche mostrate all'utente nell'app Kaspersky Endpoint Security for Android.
- Configurazione delle impostazioni nei dispositivi che supportano Samsung KNOX 2.6 o versioni successive.
- Configurazione delle impostazioni nei dispositivi che supportano i profili lavoro Android.
- Distribuzione dell'app Kaspersky Endpoint Security for Android tramite la console Samsung KNOX Mobile Enrollment. Samsung KNOX Mobile Enrollment è destinata all'installazione in batch e alla configurazione iniziale delle app nei dispositivi Samsung acquistati da fornitori ufficiali.
- Un upgrade dell'app Kaspersky Endpoint Security for Android alla versione specificata può essere eseguito utilizzando i criteri di Kaspersky Security Center.
- Le notifiche dell'amministratore sullo stato e sugli eventi dell'app Kaspersky Endpoint Security for Android possono essere comunicate in Kaspersky Security Center o tramite e-mail.
- Controllo delle modifiche per le impostazioni dei criteri (cronologia delle revisioni).

Kaspersky Security for Mobile include i seguenti componenti di gestione e protezione:

- Anti-Virus (per dispositivi Android)
- Antifurto (per dispositivi Android)
- Protezione Web (per dispositivi Android e iOS)
- Controllo app (per dispositivi Android)
- Controllo conformità (per dispositivi Android)
- Rilevamento dei privilegi di root nei dispositivi (per i dispositivi Android)

Informazioni sull'app Kaspersky Endpoint Security for Android

L'app Kaspersky Endpoint Security for Android garantisce la protezione dei dispositivi mobili da minacce Web, virus e altri programmi che rappresentano minacce.

L'app Kaspersky Endpoint Security for Android include i seguenti componenti:

- **Anti-Virus**. Consente di rilevare e neutralizzare le minacce nel dispositivo utilizzando i database anti-virus e il servizio cloud Kaspersky Security Network. Anti-Virus include i seguenti componenti:
  - Protezione. Rileva le minacce nei file aperti, esamina le nuove app e protegge in tempo reale i dispositivi dalle infezioni.
  - Scansione. Viene avviata su richiesta per l'intero file system, solo per le app installate o per un file o una cartella in particolare.
  - Aggiornamento. Aggiornamento consente all'utente di scaricare nuovi database anti-virus per l'applicazione.

- **Antifurto.** Questo componente protegge le informazioni sul dispositivo dall'accesso non autorizzato in caso di furto o smarrimento del dispositivo. Questo componente consente di inviare i seguenti comandi al dispositivo:
  - **Localizza** per ottenere le coordinate della posizione del dispositivo.
  - **Allarme** per fare in modo che il dispositivo emetta un forte allarme.
  - **Foto utente** per fare in modo che il dispositivo scatti foto con la fotocamera anteriore se qualcuno tenta di sbloccarlo.
  - **Cancella** dati aziendali per proteggere le informazioni aziendali sensibili.
- **Protezione Web.** Questo componente blocca i siti dannosi progettati per distribuire codice dannoso. Protezione Web blocca anche i siti Web contraffatti (di phishing) progettati per rubare informazioni riservate (ad esempio password di online banking o sistemi e-money) e ottenere l'accesso alle informazioni finanziarie dell'utente. Protezione Web analizza i siti Web prima dell'apertura utilizzando il servizio cloud Kaspersky Security Network. Dopo la scansione, Protezione Web consente il caricamento dei siti Web ritenuti attendibili e blocca i siti Web dannosi. Protezione Web supporta inoltre il filtro dei siti Web in base alle categorie definite nel servizio cloud Kaspersky Security Network. Questo consente all'amministratore di limitare l'accesso dell'utente a determinate categorie di pagine Web (ad esempio, alle pagine Web delle categorie "Gioco d'azzardo, lotterie, scommesse" o "Comunicazioni di rete").
- **Controllo app.** Questo componente consente di installare le app consigliate e richieste nel dispositivo tramite un collegamento diretto al pacchetto di distribuzione o tramite un collegamento a Google Play. Controllo app consente di rimuovere le app bloccate che violano i requisiti di sicurezza aziendali.
- **Controllo conformità.** Questo componente consente di verificare la conformità dei dispositivi gestiti con i requisiti di sicurezza aziendali e di imporre restrizioni su determinate funzioni dei dispositivi non conformi.

Informazioni su Kaspersky Device Management for iOS

Kaspersky Device Management for iOS garantisce la protezione e il controllo dei dispositivi mobili connessi a Kaspersky Security Center e include funzionalità di gestione dei dispositivi, tra cui:

- **Protezione tramite password**. Questa funzionalità consente di impostare i requisiti di complessità delle password in modo che gli utenti utilizzino password complesse conformi ai criteri delle password aziendali.
- **Gestione di rete**. Questa funzionalità consente di aggiungere reti VPN e Wi-Fi approvate o di limitare l'accesso agli altri.
- **Cancella dati aziendali**. In caso di furto o smarrimento del dispositivo, è possibile inviare il comando Cancella per proteggere le informazioni aziendali sensibili.
- **Protezione Web**. Questo componente blocca i siti dannosi progettati per distribuire codice dannoso. Protezione Web blocca anche i siti Web contraffatti (di phishing) progettati per rubare informazioni riservate (ad esempio password di online banking o sistemi e-money) e ottenere l'accesso alle informazioni finanziarie dell'utente. Protezione Web analizza i siti Web prima dell'apertura utilizzando il servizio cloud Kaspersky Security Network. Dopo la scansione, Protezione Web consente il caricamento dei siti Web ritenuti attendibili e blocca i siti Web dannosi. Protezione Web supporta inoltre il filtro dei siti Web in base alle categorie definite nel servizio cloud Kaspersky Security Network. Questo consente all'amministratore di limitare l'accesso dell'utente a determinate categorie di pagine Web (ad esempio, alle pagine Web delle categorie "Gioco d'azzardo, lotterie, scommesse" o "Comunicazioni di rete").
- **Restrizioni delle applicazioni.** Questo componente consente di controllare se le app native del dispositivo, come iTunes, Safari o Game Center, possono essere utilizzate in un dispositivo supervisionato.

- **Restrizioni delle funzionalità.** Questo componente consente di verificare la conformità dei dispositivi gestiti con i requisiti di sicurezza aziendali e di imporre restrizioni su determinate funzioni dei dispositivi non conformi.

Informazioni su una cassetta postale Exchange

Una *cassetta postale Exchange* è un'app client del servizio Exchange ActiveSync. L'app è progettata per consentire agli utenti aziendali di utilizzare e-mail, calendario, contatti e attività. Una cassetta postale Exchange consente di connettere un dispositivo mobile a un server Microsoft Exchange. Per maggiori informazioni sul servizio Exchange ActiveSync, visitare il *sito Web del Supporto tecnico Microsoft*.

Per gestire i dispositivi mobili utilizzando il protocollo Exchange ActiveSync, il server Exchange deve essere distribuito nel server Microsoft Exchange. Per ulteriori informazioni sull'installazione di un Exchange Server, fare riferimento alla *Guida di Kaspersky Security Center*. Non sono richieste ulteriori operazioni di configurazione nei dispositivi mobili.

Utilizzando una cassetta postale Exchange è possibile configurare in remoto i dispositivi EAS attraverso i criteri di gruppo e inviare il comando di cancellazione dei dati. I seguenti sistemi operativi supportano il protocollo Exchange ActiveSync:

- Windows Mobile
- Windows CE
- Windows Phone
- Android
- Bada
- BlackBerry 10
- iOS
- Symbian

Il set di impostazioni di gestione per un dispositivo Exchange ActiveSync dipende dal sistema operativo in esecuzione nel dispositivo mobile. Per informazioni dettagliate sulle funzionalità di supporto del protocollo Exchange ActiveSync per un sistema operativo specifico, fare riferimento alla documentazione del sistema operativo specifico.

Informazioni sul plug-in di amministrazione di Kaspersky Endpoint Security for Android

Il plug-in di amministrazione di Kaspersky Endpoint Security for Android fornisce l'interfaccia per la gestione dei dispositivi mobili e delle app mobili installate in essi tramite Administration Console di Kaspersky Security Center. Il plug-in di amministrazione di Kaspersky Endpoint Security for Android può essere utilizzato per:

- Creare criteri di sicurezza di gruppo per i dispositivi mobili.
- Configurare in remoto le impostazioni operative dell'app Kaspersky Endpoint Security for Android nei dispositivi mobili degli utenti.

- Ricevere rapporti e statistiche sul funzionamento dell'app mobile Kaspersky Endpoint Security for Android nei dispositivi degli utenti.

Il plug-in di amministrazione di Kaspersky Endpoint Security for Android è installato per impostazione predefinita durante la distribuzione di Kaspersky Security Center. Il plug-in non richiede l'installazione singola.

Informazioni sul plug-in di amministrazione di Kaspersky Device Management for iOS

Il plug-in di amministrazione di Kaspersky Device Management for iOS fornisce un'interfaccia per gestire i dispositivi mobili connessi tramite il protocollo Exchange ActiveSync e MDM iOS mediante Administration Console di Kaspersky Security Center. Il plug-in di amministrazione di Kaspersky Device Management for iOS può essere utilizzato per eseguire le seguenti operazioni:

- Creare criteri di sicurezza di gruppo per i dispositivi mobili.
- Configurare in remoto i dispositivi connessi tramite il protocollo Exchange ActiveSync (di seguito denominati "Dispositivi EAS").
- Configurare in remoto i dispositivi connessi tramite il protocollo MDM iOS (di seguito denominati "Dispositivi MDM iOS").
- Ricevere rapporti e statistiche sul funzionamento dei dispositivi mobili degli utenti.

Per informazioni dettagliate sulla connessione dei dispositivi mobili a Kaspersky Security Center con l'utilizzo dei protocolli MDM iOS e Exchange ActiveSync, fare riferimento alla *Guida di Kaspersky Security Center*.

Il plug-in di amministrazione di Kaspersky Device Management for iOS è installato per impostazione predefinita durante la distribuzione di Kaspersky Security Center. Il plug-in non richiede l'installazione separata.

Requisiti hardware e software

Questa sezione elenca i requisiti hardware e software per il computer dell'amministratore utilizzato per distribuire le app nei dispositivi mobili, nonché i sistemi operativi dei dispositivi mobili supportati da Kaspersky Security for Mobile.

Requisiti hardware e software per il computer dell'amministratore

Per distribuire la soluzione completa Kaspersky Security for Mobile, il computer dell'amministratore deve soddisfare i requisiti hardware di Kaspersky Security Center. Per ulteriori informazioni sui requisiti hardware di Kaspersky Security Center, vedere la *Guida di Kaspersky Security Center*.

Per poter funzionare con il plug-in di amministrazione di Kaspersky Endpoint Security for Android, nel computer dell'amministratore deve essere installato il componente Administration Console di Kaspersky Security Center versione 12 o successiva.

Per poter funzionare con il plug-in di amministrazione di Kaspersky Device Management for iOS, il computer dell'amministratore deve soddisfare i seguenti requisiti software:

- Administration Console di Kaspersky Security Center 12 o versioni successive

- Componente server Exchange
- Componente server MDM iOS
- Set di istruzioni della versione SSE2 o successiva

Per distribuire l'app mobile Kaspersky Endpoint Security for Android tramite Administration Server, il computer dell'amministratore deve soddisfare i seguenti requisiti software:

- Kaspersky Security Center 12 o versioni successive
- Plug-in di amministrazione di Kaspersky Endpoint Security for Android

Non sono previsti requisiti software per il computer dell'amministratore quando l'app mobile Kaspersky Endpoint Security for Android viene distribuita dai negozi online di riferimento.

L'app mobile di Kaspersky Endpoint Security for Android può essere utilizzata anche nell'ambito del sistema di amministrazione remota di Kaspersky Endpoint Security Cloud (versione 6.0 e successiva). Per ulteriori informazioni sull'utilizzo delle app tramite Kaspersky Endpoint Security Cloud, fare riferimento alla *Guida di Kaspersky Endpoint Security Cloud*.

L'app mobile di Kaspersky Endpoint Security for Android può funzionare nell'ambito di sistemi EMM di terze parti:

- VMWare AirWatch 9.3 o versione successiva
- MobileIron 10.0 o successiva
- IBM MaaS360 10.68 o versione successiva
- Microsoft Intune 1908 o versione successiva
- SOTI MobiControl 14.1.4 (1693) o successiva

Requisiti hardware e software per consentire al dispositivo mobile dell'utente di supportare l'installazione dell'app Kaspersky Endpoint Security for Android

L'app Kaspersky Endpoint Security for Android presenta i seguenti requisiti hardware e software:

- Smartphone o tablet con una risoluzione dello schermo di 320x480 pixel o superiore
- 65 MB di spazio disponibile sul disco nella memoria principale del dispositivo
- Android 5.0–12 (compreso Android 12L, a esclusione di Go Edition)
- Architettura del processore x86, x86-64, Arm5, Arm6, Arm7 o Arm8

L'app può essere installata soltanto nella memoria principale del dispositivo.

Requisiti hardware e software per un profilo MDM iOS

Per un profilo MDM iOS, il dispositivo deve soddisfare i seguenti requisiti hardware e software:

- iOS 10.0–15.0 o iPadOS 13–15

- Connessione Internet

Problemi noti e considerazioni

Kaspersky Endpoint Security for Android presenta una serie di problemi noti che non sono critici per il funzionamento dell'app.

Problemi noti durante l'installazione delle app

- Kaspersky Endpoint Security for Android viene installato solo nella memoria principale del dispositivo.
- Nei dispositivi che eseguono Android 7.0 potrebbe verificarsi un errore durante i tentativi di disabilitare i diritti di amministratore per Kaspersky Endpoint Security for Android nelle impostazioni del dispositivo se per Kaspersky Endpoint Security for Android è vietata la sovrapposizione con altre finestre. Questo problema è causato da un difetto ben noto in Android 7.
- Kaspersky Endpoint Security for Android nei dispositivi che eseguono Android 7.0 o versioni successive non supporta la modalità multi-finestra.
- Kaspersky Endpoint Security for Android non funziona nei dispositivi Chrome che eseguono il sistema operativo Chrome.
- Kaspersky Endpoint Security for Android non funziona nei dispositivi che eseguono il sistema operativo Android (Go Edition).
- Durante l'utilizzo dell'app Kaspersky Endpoint Security for Android con sistemi EMM di terze parti (ad esempio VMWare AirWatch), sono disponibili solo i componenti Anti-Virus e Protezione Web. L'amministratore può configurare le impostazioni di Anti-Virus e Protezione Web nella console di sistema EMM. In questo caso, le notifiche sul funzionamento dell'app sono disponibili solo nell'interfaccia dell'app Kaspersky Endpoint Security for Android (Rapporti).

Problemi noti durante l'upgrade della versione dell'app

- È possibile eseguire l'upgrade di Kaspersky Endpoint Security for Android solo a una versione più recente dell'app. Non è possibile eseguire il downgrade di Kaspersky Endpoint Security for Android a una versione precedente.
- Per eseguire l'upgrade di Kaspersky Endpoint Security for Android utilizzando un pacchetto di installazione indipendente, l'installazione delle app da origini sconosciute deve essere consentita nel dispositivo mobile dell'utente.
- È possibile eseguire l'aggiornamento tramite Google Play se Kaspersky Endpoint Security for Android è stato installato da Google Play. Se l'app è stata installata con un altro metodo, non è possibile eseguire l'aggiornamento tramite Google Play.
- È possibile eseguire l'aggiornamento tramite Kaspersky Security Center se Kaspersky Endpoint Security for Android è stato installato tramite Kaspersky Security Center. Se l'app è stata installata da Google Play, non è possibile aggiornare l'app tramite Kaspersky Security Center.
- In seguito all'upgrade dei plug-in di amministrazione alla versione Technical Release 33, anche l'app Kaspersky Endpoint Security for Android deve essere aggiornata alla versione Technical Release 33. In caso contrario, non sarà possibile attivare Samsung KNOX in alcuni dispositivi degli utenti.

Problemi noti durante l'esecuzione di Anti-Virus

- A causa di limitazioni tecniche, Kaspersky Endpoint Security for Android non può esaminare file con dimensioni pari o superiori a 2 GB. Durante una scansione, l'app ignora tali file senza inviare una notifica in merito.
- Per un'ulteriore analisi di un dispositivo per il rilevamento delle nuove minacce per cui non sono ancora state aggiunte informazioni ai database anti-virus, è necessario abilitare l'utilizzo di Kaspersky Security Network. *Kaspersky Security Network (KSN)* è un'infrastruttura di servizi cloud che consente l'accesso alla Knowledge Base online di Kaspersky con informazioni sulla reputazione di file, risorse Web e software. Per l'utilizzo di KSN, il dispositivo mobile deve essere connesso a Internet.
- In alcuni casi, l'aggiornamento dei database anti-virus da Administration Server in un dispositivo mobile potrebbe non andare a buon fine. In questo caso, eseguire l'attività di aggiornamento dei database anti-virus in Administration Server.
- In alcuni dispositivi Kaspersky Endpoint Security for Android non rileva dispositivi connessi tramite USB OTG. Non è possibile eseguire una scansione virus in tali dispositivi.
- Nei dispositivi che eseguono Android 11.0 o versioni successive l'utente deve concedere l'autorizzazione "Consentire l'accesso per gestire tutti i file".
- Nei dispositivi che eseguono Android 7.0 o versioni successive la finestra di configurazione per la pianificazione dell'esecuzione delle scansioni virus potrebbe essere visualizzata in modo errato (gli elementi di gestione non sono visualizzati). Questo problema è causato da un difetto ben noto in Android 7.
- Nei dispositivi con Android 7.0, la protezione in tempo reale in modalità estesa non rileva le minacce presenti nei file archiviati in una scheda SD esterna.
- Nei dispositivi che eseguono Android 6.0 Kaspersky Endpoint Security for Android non rileva il download di un file dannoso nella memoria del dispositivo. Un file dannoso può essere rilevato da Anti-Virus al momento dell'esecuzione del file o nel corso di una scansione virus del dispositivo. Questo problema è causato da un difetto ben noto in Android 6.0. Per garantire la sicurezza del dispositivo, è consigliabile configurare scansioni virus pianificate.

Problemi noti durante l'esecuzione di Protezione Web

- Protezione Web nei dispositivi Android funziona solo nel browser Google Chrome (inclusa la funzionalità Schede personalizzate), in Huawei Browser e Samsung Internet Browser. Protezione Web per Samsung Internet Browser non blocca i siti su un dispositivo mobile se viene utilizzato un profilo lavoro e Protezione Web è abilitato solo per il profilo lavoro.
- Kaspersky Endpoint Security nel profilo lavoro esamina solo il dominio dei siti Web nel traffico HTTPS. I siti Web dannosi e di phishing possono rimanere sbloccati se l'app è installata nel profilo lavoro. Se il dominio è attendibile, Protezione Web può ignorare una minaccia (ad esempio `https://trusted.domain.com/phishing/`). Se il dominio non è attendibile, Protezione Web blocca i siti Web dannosi e di phishing.
- Per il funzionamento di Protezione Web, è necessario abilitare l'utilizzo di Kaspersky Security Network. Protezione Web blocca i siti Web in base ai dati di KSN sulla reputazione e la categoria dei siti Web.
- I siti Web non consentiti potrebbero non essere bloccati da Protezione Web nei dispositivi che eseguono Android 6.0 con Google Chrome 51 (o versioni precedenti) se il sito Web viene aperto nei seguenti modi (questo problema è causato da un problema noto di Google Chrome):
  - Dai risultati di ricerca

- Dall'elenco dei segnalibri
- Dalla cronologia delle ricerche
- Utilizzando la funzione di completamento automatico degli indirizzi Web
- Aprendo il sito Web in una nuova scheda in Google Chrome

- I siti Web non consentiti potrebbero non essere bloccati in Google Chrome 50 (o versioni precedenti) se il sito Web viene aperto dalla pagina dei risultati di ricerca di Google mentre la funzionalità **Unisci schede e app** è abilitata nelle impostazioni del browser. Questo problema è causato da un difetto ben noto in Google Chrome.
- I siti Web delle categorie bloccate possono rimanere sbloccati in Google Chrome se l'utente li apre da app di terze parti, ad esempio da un'app del client IM. Questo problema è correlato alla modalità di esecuzione del servizio di accessibilità con la funzionalità Schede personalizzate di Chrome.
- I siti Web vietati possono rimanere sbloccati in Samsung Internet Browser se l'utente li apre in background dal menu di scelta rapida o da app di terze parti, ad esempio da un'app del client IM.
- Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità al fine di garantire il corretto funzionamento di Protezione Web.
- Quando si immette l'indirizzo di un sito Web nelle impostazioni di Protezione Web, attenersi alle seguenti regole:
  - Per i dispositivi Android, specificare l'indirizzo nel formato delle espressioni regolari (ad esempio, `http:\/\/www\.example\.com.*`).
  - Per i dispositivi MDM iOS, specificare il protocollo di trasporto dati HTTP o HTTPS (ad esempio, `http://www.example.com`).
- I siti Web consentiti possono essere bloccati nel browser Samsung Internet nella modalità di Protezione Web **Solo i siti Web elencati sono consentiti** quando la pagina viene aggiornata. I siti Web vengono bloccati se un'espressione regolare contiene impostazioni avanzate (ad esempio `^https?:\/\/example\.com\/pictures\/`). È consigliabile utilizzare espressioni regolari senza impostazioni aggiuntive (ad esempio `^https?:\/\/example\.com`).

Problemi noti durante l'esecuzione di Antifurto

- Per l'invio tempestivo dei comandi ai dispositivi Android, l'app utilizza il servizio Firebase Cloud Messaging (FCM). Se FCM non è configurato, i comandi verranno inviati al dispositivo solo durante la sincronizzazione con Kaspersky Security Center in base alla pianificazione definita nel criterio, ad esempio, ogni 24 ore).
- Per bloccare un dispositivo, Kaspersky Endpoint Security for Android deve essere impostato come amministratore del dispositivo.
- Per bloccare i dispositivi che eseguono Android 7.0 o versioni successive, Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità.
- In alcuni dispositivi l'esecuzione dei comandi di Antifurto può non andare a buon fine se nel dispositivo è abilitata la modalità Risparmio batteria. Questo difetto è stato confermato in Alcatel 5080X.
- Per localizzare i dispositivi che eseguono Android 10.0 o versioni successive, l'utente deve concedere l'autorizzazione "Sempre" per la localizzazione del dispositivo.
- Per scattare una foto utente con dispositivi che eseguono Android 11.0 o versioni successive, l'utente deve concedere l'autorizzazione "Durante l'utilizzo dell'app" per accedere alla fotocamera.

Problemi noti durante l'esecuzione di Controllo app

- Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità al fine di garantire il corretto funzionamento di Controllo app.
- Per il funzionamento di Controllo app (categorie di app), è necessario abilitare l'utilizzo di Kaspersky Security Network. Controllo app determina la categoria di un'app in base ai dati disponibili in KSN. Per l'utilizzo di KSN, il dispositivo mobile deve essere connesso a Internet. Per Controllo app, è possibile aggiungere singole app agli elenchi delle app bloccate e consentite. In questo caso, KSN non è necessario.
- Durante la configurazione di Controllo app, è consigliabile deselezionare la casella **Blocca app di sistema**. Il blocco delle app di sistema potrebbe generare problemi di funzionamento del dispositivo.

Problemi noti durante la configurazione della posta elettronica

- La configurazione remota di una cassetta postale è disponibile solo nei seguenti dispositivi:
  - Dispositivi MDM iOS.
  - Dispositivi Samsung (Exchange ActiveSync).
  - Dispositivi Android con il client di posta TouchDown installato

    Nelle versioni precedenti di Kaspersky Endpoint Security for Android è possibile utilizzare Kaspersky Security Center per configurare in remoto le impostazioni del profilo TouchDown nel dispositivo di un utente. Il supporto di TouchDown è stato interrotto in Kaspersky Endpoint Security for Android Service Pack 4. Per maggiori dettagli, consultare il *sito Web dell'assistenza tecnica Symantec*.

    Dopo aver eseguito l'upgrade del plug-in di Kaspersky Endpoint Security for Android, le impostazioni di TouchDown nel criterio sono nascoste, ma vengono salvate. Quando vengono connessi nuovi dispositivi, le impostazioni di TouchDown saranno configurate dopo l'applicazione del criterio.

    Una volta modificato e salvato il criterio, le impostazioni di TouchDown verranno eliminate. Le impostazioni di TouchDown nei dispositivi di un utente saranno cancellate dopo l'applicazione di un criterio.

Problemi noti durante la configurazione della complessità della password di sblocco del dispositivo

- Nei dispositivi che eseguono Android 10.0 o versioni successive Kaspersky Endpoint Security risolve i requisiti di complessità della password in uno dei valori di sistema: medio o alto.

  Se la lunghezza della password richiesta è compresa tra 1 e 4 simboli, l'app richiede all'utente di impostare una password di complessità media. Deve essere una password numerica (PIN) senza sequenze ripetute o ordinate (ad es. 1234) oppure alfanumerica. Il PIN o la password deve contenere almeno 4 caratteri.

  Se la lunghezza della password richiesta è superiore a 5 simboli, l'app richiede all'utente di impostare una password di complessità alta. Deve essere una password numerica (PIN) senza sequenze ripetute o ordinate oppure alfanumerica (password). Il PIN deve contenere almeno 8 cifre; la password deve contenere almeno 6 caratteri.

- Nei dispositivi che eseguono Android 10.0 o versioni successive l'uso dell'impronta digitale per sbloccare lo schermo può essere gestito solo per il profilo lavoro.

- Nei dispositivi che eseguono Android 7.1.1 se la password di sblocco non soddisfa i requisiti di sicurezza aziendali (Controllo conformità), l'app di sistema Impostazioni può funzionare in modo errato quando si tenta di modificare la password di sblocco tramite Kaspersky Endpoint Security for Android. Il problema è causato da un difetto ben noto in Android 7.1.1. In questo caso, per modificare la password di sblocco, utilizzare solo l'app di sistema Impostazioni.

- In alcuni dispositivi che eseguono Android 6.0 o versioni successive può verificarsi un errore quando si immette la password di sblocco dello schermo se i dati del dispositivo sono criptati. Questo problema è correlato alle specifiche funzionalità del servizio di accessibilità con il firmware MIUI.

Problemi noti durante la configurazione del Wi-Fi

- Nei dispositivi che eseguono Android 8.0 o versioni successive le impostazioni del server proxy per il Wi-Fi non possono essere ridefinite con il criterio. Tuttavia, è possibile configurare manualmente le impostazioni del server proxy per una rete Wi-Fi nel dispositivo mobile.

Problemi noti durante la configurazione di APN

- La configurazione remota dell'APN è disponibile solo nei dispositivi MDM iOS o nei dispositivi Samsung.

- Configurare l'APN per i dispositivi MDM iOS nella sezione **Comunicazioni cellulari**. La sezione **APN** non è aggiornata. Prima di configurare le impostazioni APN, verificare che la casella **Applica impostazioni nel dispositivo** nella sezione **APN** sia deselezionata.

Problemi noti con Firewall

- L'utilizzo di Firewall è disponibile solo nei dispositivi Samsung.

Problemi noti durante la configurazione della VPN

- La configurazione remota di una VPN è disponibile solo nei seguenti dispositivi:

  - Dispositivi MDM iOS.

  - Dispositivi Samsung.

Problemi noti durante l'utilizzo dei contenitori

- In Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2 non è più disponibile il supporto per la creazione di contenitori per le app mobili. Tuttavia, i contenitori creati nelle versioni precedenti dell'applicazione possono essere aggiunti ai dispositivi Android.

- Per installare app inserite in un contenitore, nel dispositivo mobile dell'utente deve essere consentita l'installazione di app da origini sconosciute. Per ulteriori informazioni sull'installazione delle app senza Google Play, fare riferimento alla *Guida Android*.

- L'inserimento delle app in contenitori non è supportato nei dispositivi Android per le app che contengono più di 65.536 metodi (configurazione multidex).

Problemi noti con la protezione dalla rimozione delle app

- Kaspersky Endpoint Security for Android deve essere impostato come amministratore del dispositivo.
- Per proteggere l'app dalla rimozione nei dispositivi che eseguono Android 7.0 o versioni successive, Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità.
- In alcuni dispositivi Xiaomi e Huawei, la protezione dalla rimozione di Kaspersky Endpoint Security for Android non funziona. Questo problema è causato da funzionalità specifiche del firmware MIUI 7 e 8 in Xiaomi e del firmware EMUI in Huawei.

Problemi noti durante la configurazione delle restrizioni relative ai dispositivi

- Nei dispositivi con Android 10.0 o versioni successive, il divieto di utilizzo delle reti Wi-Fi non è supportato.
- Nei dispositivi che eseguono Android 10.0 o versioni successive, l'utilizzo della fotocamera non può essere completamente vietato.
- Nei dispositivi che eseguono Android 11 o versioni successive Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo. In tal caso, non sarà possibile limitare l'utilizzo della fotocamera.

Problemi noti durante l'invio dei comandi ai dispositivi mobili

- Nei dispositivi che eseguono Android 12 o versioni successive, se l'utente ha concesso l'autorizzazione per l'utilizzo della posizione approssimativa, l'app Kaspersky Endpoint Security for Android cerca prima di ottenere la posizione esatta del dispositivo. Se l'operazione non va a buon fine, viene restituita la posizione approssimativa del dispositivo solo se è stata ricevuta non più di 30 minuti prima. In caso contrario, il comando di **Localizza dispositivo** non va a buon fine.

Problemi noti del profilo lavoro Android

- Se si crea un profilo lavoro Android utilizzando un criterio, l'utente deve concedere l'autorizzazione "Consentire l'accesso per gestire tutti i file" a Kaspersky Endpoint Security for Android installato nei dispositivi che eseguono Android 11 o versioni successive e associato al profilo lavoro.

Problemi noti con dispositivi specifici

- In determinati dispositivi (ad esempio Huawei, Meizu e Xiaomi), è necessario concedere a Kaspersky Endpoint Security for Android un'autorizzazione di avvio automatico o aggiungere manualmente l'app all'elenco delle app eseguite all'avvio del sistema operativo. Se l'app non viene aggiunta all'elenco, Kaspersky Endpoint Security for Android interrompe l'esecuzione di tutte le funzioni in seguito al riavvio del dispositivo mobile. Inoltre, se il dispositivo è stato bloccato, non è possibile utilizzare un comando per sbloccarlo. È possibile sbloccare il dispositivo solo utilizzando un codice di sblocco monouso.
- In alcuni dispositivi (ad esempio, Meizu e Asus) con sistema operativo Android 6.0 o versione successiva, dopo il criptaggio dei dati e il riavvio del dispositivo Android, è necessario immettere una password numerica per sbloccare il dispositivo. Se l'utente utilizza una password grafica per sbloccare il dispositivo, è necessario convertire le password grafica in una password numerica. Per maggiori informazioni sulla conversione di una

password grafica in una password numerica, fare riferimento al sito Web dell'assistenza tecnica del produttore del dispositivo mobile. Questo problema è correlato all'esecuzione del servizio per le funzionalità di accessibilità.

- In alcuni dispositivi Huawei che eseguono Android 5.X, dopo l'impostazione di Kaspersky Endpoint Security for Android come funzionalità di accessibilità potrebbe essere visualizzato un messaggio errato relativo alla mancanza dei diritti appropriati. Per nascondere questo messaggio, abilitare l'app come app protetta nelle impostazioni del dispositivo.

- In alcuni dispositivi Huawei con sistema operativo Android 5.X o 6.X, quando è abilitata la modalità Risparmio batteria per Kaspersky Endpoint Security for Android, l'utente può terminare manualmente l'app. In seguito a questa operazione, il dispositivo dell'utente diventa non protetto. Questo problema è dovuto ad alcune funzionalità del software Huawei. Per ripristinare la protezione del dispositivo, eseguire Kaspersky Endpoint Security for Android manualmente. È consigliabile disabilitare la modalità Risparmio batteria per Kaspersky Endpoint Security for Android nelle impostazioni del dispositivo.

- Nei dispositivi Huawei con firmware EMUI che eseguono Android 7.0 l'utente può nascondere la notifica relativa allo stato di protezione di Kaspersky Endpoint Security for Android. Questo problema è dovuto ad alcune funzionalità del software Huawei.

- In alcuni dispositivi Xiaomi, impostando una lunghezza della password superiore a 5 caratteri in un criterio, all'utente verrà richiesto di modificare la password di sblocco dello schermo invece del codice PIN. Non è possibile impostare un codice PIN con più di 5 caratteri. Questo problema è dovuto ad alcune funzionalità del software Xiaomi.

- Nei dispositivi Xiaomi con firmware MIUI che eseguono Android 6.0 l'icona di Kaspersky Endpoint Security for Android può essere nascosta nella barra di stato. Questo problema è dovuto ad alcune funzionalità del software Xiaomi. È consigliabile consentire la visualizzazione delle icone di notifica nelle impostazioni delle notifiche.

- In alcuni dispositivi Nexus che eseguono Android 6.0.1, i privilegi richiesti per il corretto funzionamento non possono essere concessi attraverso l'Avvio rapido guidato di Kaspersky Endpoint Security for Android. Il problema è causato da un difetto ben noto della patch di protezione per Android di Google. Per garantire il corretto funzionamento, è necessario concedere manualmente i privilegi richiesti nelle impostazioni del dispositivo.

- In alcuni dispositivi Samsung con Android 7.0 o versioni successive, quando l'utente tenta di configurare metodi non supportati per lo sblocco del dispositivo (ad esempio, una password grafica), il dispositivo può essere bloccato se vengono soddisfatte le seguenti condizioni: la protezione dalla rimozione di Kaspersky Endpoint Security for Android è abilitata e sono impostati requisiti per la complessità della password di sblocco dello schermo. Per sbloccare il dispositivo, è necessario inviare un comando speciale al dispositivo.

- In determinati dispositivi Samsung, non è possibile impedire l'utilizzo delle impronte digitali per lo sblocco dello schermo.

- Protezione Web non può essere abilitato in alcuni dispositivi Samsung se il dispositivo è connesso a una rete 3G/4G, se è abilitata la modalità Risparmio batteria e vengono limitati i dati in background. È consigliabile disabilitare la funzione che limita i processi in background nelle impostazioni di Risparmio batteria.

- In determinati dispositivi Samsung, se la password di sblocco non è conforme ai requisiti di sicurezza aziendali, Kaspersky Endpoint Security for Android non impedisce l'utilizzo delle impronte digitali per lo sblocco dello schermo.

- Dopo l'esecuzione dei comandi di Antifurto (ad esempio, Localizza, Blocca dispositivo, Sblocca e Foto utente), il certificato generale e il certificato VPN possono essere eliminati in alcuni dispositivi Samsung. Per continuare è necessario reinstallare i certificati. Questo problema è dovuto allo standard di sicurezza MDFPP (Mobile Device Fundamentals Protection Profile).

- In alcuni dispositivi Honor e Huawei, non è possibile limitare l'utilizzo del Bluetooth. Quando Kaspersky Endpoint Security for Android tenta di limitare l'uso del Bluetooth, il sistema operativo visualizza una notifica contenente

le opzioni per rifiutare o consentire la limitazione. L'utente può rifiutare questa limitazione e continuare a utilizzare il Bluetooth.

- In alcuni dispositivi Samsung, dopo l'installazione o l'aggiornamento di Kaspersky Endpoint Security da un pacchetto di installazione indipendente, l'attivazione del profilo MDM KNOX non è disponibile.

- Nei dispositivi Blackview l'utente può cancellare la memoria per l'app Kaspersky Endpoint Security for Android. Di conseguenza, la protezione e la gestione del dispositivo vengono disabilitate, tutte le impostazioni definite perdono validità e l'app Kaspersky Endpoint Security for Android viene rimossa dalle funzionalità di accessibilità. Questo avviene perché i dispositivi di questo fornitore contengono l'app Recent screens personalizzata con privilegi elevati. Questa app può sovrascrivere le impostazioni di Kaspersky Endpoint Security for Android e non può essere sostituita perché fa parte del sistema operativo Android.

- In alcuni dispositivi con Android 11, l'app Kaspersky Endpoint Security for Android si arresta in modo anomalo subito dopo l'avvio. Questo problema è causato da un difetto ben noto in Android 11.

Distribuzione

Questa sezione della Guida è destinata agli specialisti che installano Kaspersky Security for Mobile, nonché agli specialisti che forniscono assistenza tecnica alle organizzazioni che utilizzano Kaspersky Security for Mobile.

Architettura della soluzione

Kaspersky Security for Mobile include i seguenti componenti:

- App mobile Kaspersky Endpoint Security for Android

  L'app Kaspersky Endpoint Security for Android garantisce la protezione dei dispositivi mobili da minacce Web, virus e altri programmi che rappresentano minacce. Supporta l'interazione tra il dispositivo mobile e Kaspersky Security Center Administration Server utilizzando Firebase Cloud Messaging.

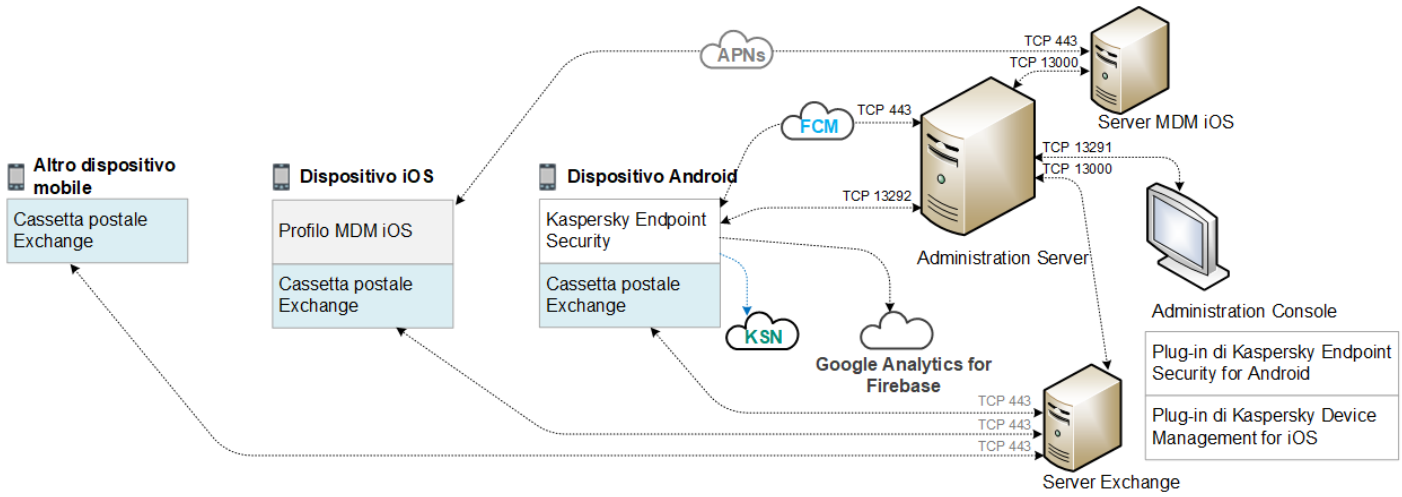
- Plug-in di amministrazione di Kaspersky Endpoint Security for Android.

  Il plug-in di amministrazione di Kaspersky Endpoint Security for Android fornisce l'interfaccia per la gestione dei dispositivi mobili e delle app mobili installate in essi tramite Administration Console di Kaspersky Security Center.

- Plug-in di amministrazione di Kaspersky Device Management for iOS

  Il plug-in di amministrazione di Kaspersky Device Management for iOS fornisce un'interfaccia per gestire i dispositivi mobili connessi tramite il protocollo Exchange ActiveSync e MDM iOS mediante Administration Console di Kaspersky Security Center.

L'architettura della soluzione integrata Kaspersky Security for Mobile è visualizzata nella figura seguente.



L'architettura di Kaspersky Security for Mobile

Per informazioni dettagliate su Administration Console, Administration Server, server Exchange e Server per dispositivi mobili MDM iOS, fare riferimento alla *Guida di Kaspersky Security Center*.

Scenari di distribuzione comuni della soluzione integrata

Questa sezione illustra gli scenari di distribuzione comuni per la soluzione integrata Kaspersky Security for Mobile.

Per distribuire la soluzione integrata nei dispositivi Android e nei dispositivi iOS è possibile utilizzare diversi scenari di distribuzione. Se l'organizzazione utilizza dispositivi mobili che eseguono diversi sistemi operativi, è necessario installare le app separatamente per ciascun sistema operativo in base allo scenario di distribuzione appropriato.

Scenari di distribuzione per Kaspersky Endpoint Security for Android

Esistono diversi modi per distribuire Kaspersky Endpoint Security for Android nei dispositivi mobili all'interno della rete aziendale. È possibile utilizzare lo scenario di distribuzione più adatto all'organizzazione oppure combinare diversi scenari di distribuzione.

Per informazioni dettagliate sulla distribuzione di Kaspersky Endpoint Security for Android in Kaspersky Endpoint Security Cloud, fare riferimento alla *Guida di Kaspersky Endpoint Security Cloud*.

Distribuzione di Kaspersky Endpoint Security for Android tramite Kaspersky Security Center

È possibile distribuire Kaspersky Endpoint Security for Android tramite Kaspersky Security Center attraverso i seguenti metodi:

- Invio di messaggi con il collegamento a Google Play (opzione consigliata)
- Inviando messaggi con un collegamento al pacchetto di app indipendente

La distribuzione di Kaspersky Endpoint Security for Android tramite Google Play consiste nell'invio di messaggi che contengono il collegamento a Google Play agli utenti dei dispositivi da Administration Console.

La distribuzione di Kaspersky Endpoint Security for Android tramite pacchetto indipendente consiste nell'esecuzione dei seguenti passaggi da parte dell'amministratore:

1. Creazione del pacchetto di installazione di un'app.
2. Configurazione delle impostazioni del pacchetto di installazione.
3. Creazione di un pacchetto di installazione indipendente.
4. Invio di messaggi con un collegamento per il download di un pacchetto di installazione indipendente agli utenti dei dispositivi Android. È disponibile l'invio di messaggi di massa.

L'utente installa Kaspersky Endpoint Security for Android in un dispositivo mobile dopo la ricezione di un messaggio con un collegamento a Google Play o un collegamento per il download del pacchetto di installazione dal server Web di Kaspersky Security Center. Non è necessaria alcuna preparazione aggiuntiva per cominciare a utilizzare l'app.

Distribuzione di Kaspersky Endpoint Security for Android da Google Play

Se l'installazione remota non è possibile, è consigliabile utilizzare lo scenario di distribuzione di Google Play.

Kaspersky Endpoint Security for Android viene installato da Google Play indipendentemente dagli utenti dei dispositivi. Gli utenti scaricano il pacchetto di distribuzione dell'app mobile da Google Play e installano l'app nei dispositivi. Dopo l'installazione dell'app nel dispositivo, è necessaria una preparazione aggiuntiva prima di poterla utilizzare: configurare le impostazioni della connessione ad Administration Server e installare un certificato generale.

Distribuzione di Kaspersky Endpoint Security for Android tramite KNOX Mobile Enrollment

La distribuzione di Kaspersky Endpoint Security for Android consiste nell'aggiunta del profilo MDM KNOX ai dispositivi mobili. Il profilo MDM KNOX contiene un collegamento a un'app distribuita nel server Web di Kaspersky Security Center o in un altro server. Dopo aver installato l'app nel dispositivo mobile, è necessario installare anche un certificato generale.

Le informazioni sull'installazione tramite KNOX Mobile Enrollment sono disponibili nella sezione Samsung KNOX.

Scenari di distribuzione per il profilo MDM iOS

Un *profilo MDM iOS* è un profilo che contiene le impostazioni per la connessione dei dispositivi mobili con sistema operativo iOS a Kaspersky Security Center. Dopo l'installazione di un profilo MDM iOS e la sincronizzazione con Kaspersky Security Center, il dispositivo diventa un dispositivo gestito. I dispositivi mobili vengono gestiti attraverso il servizio APN (Apple Push Notification). Per maggiori dettagli sull'installazione di un profilo MDM iOS e sull'utilizzo degli APNs, fare riferimento alla *Guida di Kaspersky Security Center*.

Utilizzando un profilo MDM iOS è possibile eseguire le seguenti operazioni:

- Configurare in remoto le impostazioni dei dispositivi MDM iOS utilizzando i criteri di gruppo.
- Inviare comandi di blocco del dispositivo e cancellazione dei dati.
- Installare in remoto le app di Kaspersky e altre app di terze parti.

Esistono diversi modi per distribuire un profilo MDM iOS nei dispositivi mobili all'interno della rete aziendale. È possibile utilizzare lo scenario di distribuzione più adatto all'organizzazione oppure combinare diversi scenari di distribuzione.

Prima di distribuire un profilo MDM iOS, l'amministratore deve eseguire le seguenti operazioni:

1. Installare un server MDM iOS.
2. Ottenere un certificato APN (Apple Push Notification).
3. Installare un certificato APN nel server MDM iOS.

Per maggiori dettagli sull'installazione di un server MDM iOS e sull'utilizzo di un certificato APNs, fare riferimento alla *Guida di Kaspersky Security Center*.

Per informazioni dettagliate sulla distribuzione di un profilo MDM iOS in Kaspersky Endpoint Security Cloud, fare riferimento alla *Guida di Kaspersky Endpoint Security Cloud*.

Distribuzione di un profilo MDM iOS tramite Kaspersky Security Center

La distribuzione di un profilo MDM iOS tramite Kaspersky Security Center può essere eseguita inviando messaggi che contengono un collegamento per il download del profilo MDM iOS. È disponibile l'invio di messaggi di massa.

L'utente installa il profilo MDM iOS in un dispositivo mobile dopo la ricezione del messaggio con un collegamento al server Web di Kaspersky Security Center. Non è richiesta nessuna preparazione aggiuntiva per il profilo MDM iOS.

Per maggiori dettagli sulla creazione di un profilo MDM iOS, fare riferimento alla *Guida di Kaspersky Security Center*.

Preparazione di Administration Console per la distribuzione della soluzione integrata

Questa sezione fornisce istruzioni per la preparazione di Administration Console alla distribuzione della soluzione integrata.

Configurazione delle impostazioni di Administration Server per la connessione dei dispositivi mobili

Per consentire ai dispositivi mobili di connettersi ad Administration Server, prima di installare l'app mobile Kaspersky Endpoint Security, configurare le impostazioni di connessione dei dispositivi mobili nelle proprietà di Administration Server.

Per configurare le impostazioni di Administration Server per la connessione dei dispositivi mobili:

1. Dal menu di scelta rapida di Administration Server selezionare **Proprietà**.

   Verrà visualizzata la finestra delle impostazioni di Administration Server.

2. Selezionare **Impostazioni di connessione del server** → **Porte aggiuntive**.
3. Selezionare la casella di controllo **Apri porta per i dispositivi mobili**.
4. Nel campo **Porta per dispositivi mobili** specificare la porta tramite la quale i dispositivi mobili si connetteranno all'Administration Server.

Per impostazione predefinita, viene utilizzata la porta 13292. Se la casella **Apri porta per i dispositivi mobili** è deselezionata o è specificata una porta di connessione errata, i dispositivi mobili non saranno in grado di connettersi all'Administration Server.

5. Nel campo **Porta per l'attivazione dei client mobili** specificare la porta che verrà utilizzata dai dispositivi mobili per la connessione ad Administration Server per l'attivazione dell'app Kaspersky Endpoint Security for Android. Per impostazione predefinita, viene utilizzata la porta 17100.

6. Fare clic su **OK**.

Visualizzazione della cartella Mobile Device Management in Administration Console

Visualizzando la cartella **Mobile Device Management** in Administration Console, è possibile visualizzare l'elenco dei dispositivi mobili gestiti tramite Administration Server, configurare le impostazioni di gestione dei dispositivi mobili e installare i certificati nei dispositivi mobili degli utenti.

*Per abilitare la visualizzazione della cartella **Mobile Device Management** in Administration Console:*

1. Dal menu di scelta rapida di Administration Server selezionare **Visualizzazione → Configurazione interfaccia**.

2. Nella finestra visualizzata selezionare la casella **Visualizza Mobile Device Management**.

3. Fare clic su **OK**.

La cartella **Mobile Device Management** viene visualizzata nella struttura di Administration Console in seguito al riavvio di Administration Console.

Creazione di un gruppo di amministrazione

Per eseguire la configurazione centralizzata dell'app Kaspersky Endpoint Security for Android installata nei dispositivi mobili degli utenti, è necessario applicare i criteri di gruppo ai dispositivi.

Per applicare il criterio a un gruppo di dispositivi, è consigliabile creare un gruppo distinto per tali dispositivi in **Dispositivi gestiti** prima di installare le app mobili nei dispositivi degli utenti.

Dopo la creazione di un gruppo di amministrazione, è consigliabile configurare l'opzione per l'assegnazione automatica dei dispositivi in cui si desidera installare le app a questo gruppo. Configurare quindi le impostazioni comuni a tutti i dispositivi utilizzando un criterio di gruppo.

Per creare un gruppo di amministrazione, eseguire le seguenti operazioni:

1. Nella struttura della console aprire la cartella **Dispositivi gestiti**.

2. Nell'area di lavoro della cartella o sottocartella **Dispositivi gestiti** selezionare la scheda **Dispositivi**.

3. Fare clic sul pulsante **Nuovo gruppo**.

   Verrà visualizzata la finestra in cui è possibile creare un nuovo gruppo.

4. Nella finestra **Nome del gruppo** digitare il nome del gruppo e fare clic su **OK**.

Una nuova cartella per il gruppo di amministrazione con il nome specificato verrà visualizzata nella struttura della console. Per informazioni dettagliate sull'utilizzo dei gruppi di amministrazione, vedere la *Guida di Kaspersky Security Center*.

Creazione di una regola per l'assegnazione automatica dei dispositivi ai gruppi di amministrazione

È possibile gestire in modo centralizzato le impostazioni dell'app Kaspersky Endpoint Security for Android installata nei dispositivi mobili degli utenti solo se i dispositivi appartengono a un gruppo di amministrazione creato precedentemente per il quale è stato configurato un criterio di gruppo.

Se la regola per l'assegnazione automatica al gruppo di amministrazione dei dispositivi mobili rilevati nella rete non è stata configurata, durante la prima sincronizzazione con Administration Server, il dispositivo viene automaticamente inviato alla cartella **Avanzate** → **Polling della rete** → **Domini** → **KES10**. Un criterio di gruppo non si applica a questo dispositivo.

Per creare la regola per l'assegnazione automatica dei dispositivi mobili al gruppo di amministrazione, eseguire le seguenti operazioni:

1. Nella struttura della console aprire la cartella **Dispositivi non assegnati**.
2. Nel menu di scelta rapida della cartella **Dispositivi non assegnati** selezionare **Proprietà**.

   Verrà visualizzata la finestra **Proprietà Dispositivi non assegnati**.
3. Nella sezione **Sposta dispositivi** fare clic su **Aggiungi** per avviare il processo di creazione di una regola per l'allocazione automatica dei dispositivi a un gruppo di amministrazione.

   Verrà visualizzata la finestra **Nuova regola**.
4. Digitare il nome della regola.
5. Specificare il gruppo di amministrazione al quale devono essere assegnati i dispositivi mobili dopo l'installazione dell'app mobile Kaspersky Endpoint Security for Android. A tale scopo, fare clic su **Sfoglia** a destra del campo **Gruppo in cui spostare i dispositivi** e selezionare il gruppo nella finestra visualizzata.
6. Nella sezione **Applicazione regola** selezionare **Esegui una volta per ciascun dispositivo**.
7. Selezionare la casella **Sposta solo dispositivi non aggiunti a gruppi** di amministrazione per impedire l'assegnazione al gruppo selezionato dei dispositivi mobili assegnati ad altri gruppi di amministrazione al momento dell'applicazione della regola.
8. Selezionare la casella **Abilita regola** per applicare la regola ai nuovi dispositivi rilevati.
9. Aprire la sezione **App** e procedere come segue:

   a. Selezionare la casella **Versione del sistema operativo**.

   b. Selezionare uno o più tipi di sistemi operativi dei dispositivi da assegnare al gruppo specificato: Android o iOS.
10. Fare clic su **OK**.

La nuova regola creata viene visualizzata nell'elenco delle regole di allocazione dei dispositivi nella sezione **Sposta dispositivi** della finestra delle proprietà della cartella **Dispositivi non assegnati**.

In base alla regola, Kaspersky Security Center assegna tutti i dispositivi che soddisfano i requisiti specificati dalla cartella **Dispositivi non assegnati** al gruppo selezionato. I dispositivi mobili assegnati in precedenza alla cartella **Dispositivi non assegnati** possono anche essere assegnati manualmente al gruppo di amministrazione desiderato della cartella **Dispositivi gestiti**. Per informazioni dettagliate sulla gestione dei gruppi di amministrazione e sulle azioni per i dispositivi non distribuiti, vedere la *Guida di Kaspersky Security Center*.

Creazione di un certificato generale

È necessario creare un certificato generale in Administration Console allo scopo di identificare l'utente di un dispositivo mobile.

Per creare un certificato generale:

1. Nella struttura della console selezionare la cartella **Mobile Device Management** → **Certificati**.
2. Nell'area di lavoro della cartella **Certificati** fare clic sul pulsante **Aggiungi certificato** per avviare l'Installazione guidata certificato.
3. Nella finestra **Tipo di certificato** della procedura guidata selezionare l'opzione **Certificato generale**.
4. Nella finestra **Selezione utente** della procedura guidata specificare l'utente per cui si desidera creare un certificato generale.
5. Nella finestra **Origine certificato** della procedura guidata selezionare il metodo per la creazione del certificato generale.
   - Per creare automaticamente un certificato generale utilizzando gli strumenti di Administration Server, selezionare **Emetti il certificato utilizzando gli strumenti di Administration Server**.
   - Per assegnare a un utente un certificato creato in precedenza, selezionare l'opzione **Specifica un file di certificato**. Fare clic sul pulsante **Specifica** per aprire la finestra **Certificato** e specificare il file di certificato.

     Deselezionare la casella **Pubblica certificato** se non si desidera specificare il tipo di dispositivo mobile e il metodo per la notifica all'utente della creazione del certificato.
6. Nella finestra **Metodo di notifica all'utente** della procedura guidata configurare le impostazioni per la notifica all'utente del dispositivo mobile della creazione del certificato tramite un messaggio di testo o tramite e-mail.
7. Nella finestra **Generazione del certificato** della procedura guidata fare clic su **Fine** per completare l'Installazione guidata certificato.

Come risultato, l'Installazione guidata certificato crea un certificato generale che l'utente può installare nel dispositivo mobile. Per ottenere il certificato, avviare la sincronizzazione del dispositivo mobile con l'Administration Server. Per maggiori informazioni sulla creazione dei certificati e sulla configurazione delle regole per la relativa emissione, fare riferimento alla *Guida di Kaspersky Security Center*.

Installazione di Kaspersky Endpoint Security for Android

Questa sezione descrive i metodi per la distribuzione di Kaspersky Endpoint Security for Android in una rete aziendale.

Autorizzazioni

Per tutte le funzionalità delle app, Kaspersky Endpoint Security for Android richiede all'utente le autorizzazioni richieste. Kaspersky Endpoint Security for Android richiede le autorizzazioni obbligatorie durante il completamento dell'Installazione guidata, nonché dopo l'installazione per utilizzare le singole funzionalità delle app. È impossibile installare Kaspersky Endpoint Security for Android senza concedere le autorizzazioni obbligatorie.

In determinati dispositivi (ad esempio Huawei, Meizu e Xiaomi), è necessario aggiungere manualmente Kaspersky Endpoint Security for Android all'elenco delle app eseguite all'avvio del sistema operativo nelle impostazioni del dispositivo. Se l'app non viene aggiunta all'elenco, Kaspersky Endpoint Security for Android interrompe l'esecuzione di tutte le funzioni in seguito al riavvio del dispositivo mobile.

Nei dispositivi con Android 11 o versioni successive è necessario disabilitare l'impostazione di sistema **Rimuovi le autorizzazioni se l'app non viene utilizzata**. In caso contrario, dopo che l'app non viene utilizzata per alcuni mesi il sistema ripristina automaticamente le autorizzazioni che l'utente ha concesso all'app.

Non è più disponibile il supporto per Filtro chiamate/messaggi di testo o SIM Watch in Kaspersky Endpoint Security for Android Service Pack 4 Update 4 (Build 10.8.0.103). In questo caso Kaspersky Endpoint Security for Android non richiede all'utente le autorizzazioni per la gestione degli SMS. Per abilitare Filtro chiamate/messaggi di testo e tutte le funzionalità di SIM Watch è necessario utilizzare una versione precedente di Kaspersky Endpoint Security for Android.

Autorizzazioni richieste da Kaspersky Endpoint Security for Android

Autorizzazione	Funzione dell'app
Telefono (richiesta solo per Android 5.0 – 9.X)	Connessione a Kaspersky Security Center (ID dispositivo)
Memoria (obbligatorio)	Anti-Virus
Accesso per gestire tutti i file	Anti-Virus (solo per Android 11 o versioni successive)
Dispositivi Bluetooth nelle vicinanze (per Android 12 o versioni successive)	Limita l'uso del Bluetooth
Amministratore dispositivo (obbligatoria)	Antifurto - blocco del dispositivo (solo per Android 5.0 – 6.X)
	Antifurto - foto utente con la fotocamera anteriore
	Antifurto - riproduzione di un allarme
	Antifurto - ripristino completo
	Protezione tramite password
	Protezione dalla rimozione dell'app
	Installazione del certificato di sicurezza
	Controllo app
	Gestione KNOX (solo per i dispositivi Samsung)
	Configurazione del Wi-Fi
	Configurazione di Exchange ActiveSync
	Limitazione dell'utilizzo di fotocamera, Bluetooth e Wi-Fi
Fotocamera	Antifurto - foto utente con la fotocamera anteriore

	Nei dispositivi che eseguono Android 11.0 o versioni successive, l'utente deve concedere l'autorizzazione "Durante l'utilizzo dell'app" quando richiesto.
Posizione	Antifurto - localizzazione del dispositivo Nei dispositivi che eseguono Android 10.0 o versioni successive l'utente deve concedere l'autorizzazione "Sempre" quando richiesto.
Accessibilità	Antifurto - blocco del dispositivo (solo per Android 7.0 o versione successiva)
	Protezione Web
	Controllo app
	Protezione dalla rimozione dell'app (solo per Android 7.0 o versione successiva)
	Visualizzazione degli avvisi di Kaspersky Endpoint Security for Android (solo per Android 10.0 o versione successiva)
	Limitazione dell'utilizzo della fotocamera (solo per Android 11 o versioni successive)

Installazione di Kaspersky Endpoint Security per Android utilizzando un collegamento a Google Play

Kaspersky Endpoint Security for Android viene installato nei dispositivi mobili degli utenti i cui account utente sono stati aggiunti in Kaspersky Security Center. Per maggiori informazioni sugli account utente in Kaspersky Security Center, fare riferimento alla Guida di Kaspersky Security Center.

Kaspersky Security for Mobile consente di installare l'app tramite Kaspersky Security Center utilizzando un collegamento a Google Play (metodo consigliato).

L'utente riceverà un collegamento a Google Play. L'app può essere installata seguendo la procedura di installazione standard nella piattaforma Android. Non sono richieste ulteriori operazioni di configurazione di Kaspersky Endpoint Security for Android dopo l'installazione.

Alcuni dispositivi Huawei e Honor non dispongono dei servizi Google e quindi dell'accesso alle app in Google Play. Se alcuni utenti di dispositivi Huawei e Honor non possono installare l'app da Google Play, dovrebbero ricevere indicazione di installare l'app da Huawei App Gallery.

Il collegamento contiene i seguenti dati:

- Impostazioni di sincronizzazione di Kaspersky Security Center.
- Certificato generale.

- Indicatore di accettazione dei termini e delle condizioni del Contratto di licenza con l'utente finale per Kaspersky Endpoint Security for Android e di informative aggiuntive. Se l'amministratore accetta i termini del Contratto di licenza e di informative aggiuntive in Administration Console, Kaspersky Endpoint Security for Android ignora il passaggio di accettazione durante l'installazione dell'app.

Per installare Kaspersky Endpoint Security for Android tramite Kaspersky Security Center utilizzando un collegamento a Google Play:

1. Nella struttura della console selezionare la cartella **Mobile Device Management → Dispositivi mobili**.

2. Nell'area di lavoro della cartella **Dispositivi mobili** fare clic sul pulsante **Aggiungi dispositivo mobile**.

   Verrà avviata la procedura guidata per la connessione di un nuovo dispositivo mobile. Seguire le istruzioni della procedura guidata.

3. Nella finestra **Sistema operativo** della procedura guidata selezionare **Android**.

   Kaspersky Security Center verifica la disponibilità di aggiornamenti del plug-in di amministrazione. Se Kaspersky Security Center rileva aggiornamenti, è possibile installare la nuova versione del plug-in di amministrazione. Quando il plug-in di amministrazione viene aggiornato, è possibile accettare i termini e le condizioni del Contratto di licenza con l'utente finale e di informative aggiuntive per Kaspersky Endpoint Security for Android. Se l'amministratore accetta il Contratto di licenza e informative aggiuntive in Administration Console, Kaspersky Endpoint Security for Android ignora il passaggio di accettazione durante l'installazione dell'app. Questa funzionalità è disponibile in Kaspersky Security Center versione 12.

4. Nella pagina del **metodo di installazione di Kaspersky Endpoint Security for Android** selezionare il metodo di installazione dell'app **Utilizzando un collegamento a Google Play**.

5. Nella finestra **Seleziona utenti** della procedura guidata selezionare uno o più utenti per l'installazione di Kaspersky Endpoint Security for Android nei relativi dispositivi mobili.

   Se un utente non è nell'elenco, è possibile aggiungere un nuovo account utente senza uscire dalla procedura guidata per la connessione di un nuovo dispositivo mobile.

6. Nella pagina **Origine certificato** della procedura guidata selezionare l'origine del certificato per la protezione del trasferimento dei dati tra Kaspersky Endpoint Security for Android e Kaspersky Security Center:

   - **Rilasciare il certificato attraverso gli strumenti di Administration Server.** In questo caso, il certificato verrà creato automaticamente.

   - **Specificare il file di certificato**. In questo caso, il certificato deve essere preparato per tempo ed essere successivamente selezionato nella finestra della procedura guidata. Questa opzione non può essere utilizzata se si desidera installare Kaspersky Endpoint Security for Android in più dispositivi mobili. È necessario creare un certificato distinto per ogni utente.

7. Nella pagina **Metodo di notifica all'utente** della procedura guidata selezionare il canale utilizzato per inoltrare il collegamento per l'installazione dell'app:

   - Per inviare il collegamento tramite e-mail, selezionare **Invia collegamento a Kaspersky Endpoint Security** e configurare le impostazioni nella sezione **Tramite e-mail**. Accertarsi che l'indirizzo e-mail sia specificato nelle impostazioni degli account utente.

   - Per inviare il collegamento tramite messaggio SMS, selezionare **Invia collegamento a Kaspersky Endpoint Security** e configurare le impostazioni nella sezione **Tramite SMS**. Accertarsi che il numero di telefono sia specificato nelle impostazioni degli account utente.

   - Per installare Kaspersky Endpoint Security for Android utilizzando un codice QR, selezionare **Mostra collegamento al pacchetto di installazione** ed esaminare il codice QR utilizzando la fotocamera del dispositivo mobile.

- Se nessuno dei metodi elencati è idoneo, selezionare **Mostra collegamento al pacchetto di installazione** → **Copia** per copiare il collegamento per l'installazione di Kaspersky Endpoint Security for Android negli Appunti. Utilizzare qualsiasi metodo disponibile per inviare il collegamento per l'installazione dell'app. È inoltre possibile utilizzare altri metodi di installazione di Kaspersky Endpoint Security for Android.

8. Fare clic su **Fine** per chiudere la procedura guidata per la connessione di un nuovo dispositivo mobile.

Dopo l'installazione di Kaspersky Endpoint Security for Android nei dispositivi mobili degli utenti, sarà possibile configurare le impostazioni per dispositivi e app utilizzando i criteri di gruppo. Sarà inoltre possibile inviare comandi ai dispositivi mobili per la protezione dei dati in caso di furto o smarrimento dei dispositivi.

Altri metodi di installazione di Kaspersky Endpoint Security for Android

È possibile installare Kaspersky Endpoint Security for Android utilizzando un collegamento al proprio server Web oppure chiedere agli utenti di installare manualmente l'app.

Installazione manuale da Google Play o Huawei AppGallery

Gli utenti possono installare manualmente Kaspersky Endpoint Security for Android da Google Play o Huawei AppGallery. L'app può essere installata seguendo la procedura di installazione standard della piattaforma Android. Gli utenti possono utilizzare i propri account Google per installare l'applicazione.

Per informazioni dettagliate sulla procedura di installazione di Kaspersky Endpoint Security for Android da Google Play, vedere il sito Web dell'assistenza tecnica di Google.

Per informazioni dettagliate sulla procedura di installazione di Kaspersky Endpoint Security for Android da Huawei AppGallery, consultare il sito Web del supporto HUAWEI.

Alcuni dispositivi Huawei e Honor non dispongono dei servizi Google e quindi dell'accesso alle app in Google Play. Se alcuni utenti di dispositivi Huawei e Honor non possono installare l'app da Google Play, dovrebbero ricevere indicazione di installare l'app da Huawei App Gallery.

Dopo aver installato Kaspersky Endpoint Security for Android da Google Play o Huawei AppGallery, è necessario predisporre l'app all'utilizzo. Il processo di preparazione dell'app per l'utilizzo include i seguenti passaggi:

1. L'amministratore invia le impostazioni di sincronizzazione dei dispositivi mobili con Administration Server (indirizzo del server e numero di porta) utilizzando qualsiasi metodo disponibile (ad esempio inviando un messaggio e-mail).

2. L'utente può configurare le impostazioni di sincronizzazione dei dispositivi mobili con Administration Server durante l'esecuzione della procedura guidata di configurazione iniziale o nelle impostazioni di Kaspersky Endpoint Security for Android.

3. L'amministratore crea un certificato generale per l'utente del dispositivo mobile.

4. L'utente riceve una notifica automatica con la richiesta di installazione del certificato generale. Quando l'installazione viene confermata, il certificato generale viene installato nel dispositivo mobile.

L'accesso a Internet deve essere abilitato nel dispositivo mobile per la sincronizzazione con Administration Server.

Vedere la Guida di Kaspersky Security Center per informazioni dettagliate su come configurare le impostazioni di sincronizzazione dei dispositivi mobili con Administration Server e ricevere un certificato generale.

Durante la successiva sincronizzazione del dispositivo mobile con Administration Server, il dispositivo mobile dell'utente in cui è installato Kaspersky Endpoint Security for Android viene spostato nella cartella **Avanzate** → **Polling della rete** → **Domini** nel gruppo di amministrazione specificato durante l'installazione dell'applicazione (il gruppo predefinito è **KES10**). È possibile spostare un dispositivo mobile nel gruppo di amministrazione creato nella cartella Dispositivi gestiti manualmente o utilizzando le regole per l'assegnazione automatica.

Questo metodo di installazione è comodo se si desidera installare una versione specifica di Kaspersky Endpoint Security for Android.

Per installare Kaspersky Endpoint Security for Android utilizzando un collegamento al proprio server Web:

1. Creare un pacchetto di installazione e configurare le relative impostazioni.

   Il *pacchetto di installazione* è un set di file creato per l'installazione remota dell'app Kaspersky tramite Kaspersky Security Center.

2. Creare un pacchetto di installazione indipendente.

   Un *pacchetto di installazione indipendente* è il file di installazione di un'app per dispositivi mobili che contiene le impostazioni di connessione dell'app ad Administration Server e un indicatore di accettazione dei termini e delle condizioni del Contratto di licenza con l'utente finale per Kaspersky Endpoint Security for Android. Viene creato sulla base del pacchetto di installazione di Kaspersky Endpoint Security for Android. Il pacchetto di installazione indipendente è una tipologia particolare di pacchetto di installazione.

L'utente riceverà un collegamento al server Web che ospita il pacchetto di installazione indipendente per Kaspersky Endpoint Security for Android. Per installare l'app, l'utente deve eseguire il file APK. Non sono richieste ulteriori operazioni di configurazione di Kaspersky Endpoint Security for Android dopo l'installazione.

Per installare Kaspersky Endpoint Security for Android utilizzando un collegamento al server Web, l'installazione delle app da origini sconosciute deve essere consentita nel dispositivo mobile dell'utente.

Creazione e configurazione di un pacchetto di installazione

Il pacchetto di installazione di Kaspersky Endpoint Security for Android è l'archivio autoestraente `sc_package.exe`. L'archivio include i file richiesti per installare le app mobili nei dispositivi:

- `adb.exe`, `AdbWinApi.dll`, `AdbWinUsbApi.dll`: un gruppo di file necessari per l'installazione di Kaspersky Endpoint Security for Android.
- `installer.ini`: file di configurazione che contiene le impostazioni di connessione ad Administration Server.
- `KES10_xx_xx_xxx.apk`: file di installazione per Kaspersky Endpoint Security for Android.
- `kmlisten.exe`: utilità per la distribuzione del pacchetto di installazione dell'applicazione tramite workstation.
- `kmlisten.ini`: file di configurazione che contiene le impostazioni per l'utilità di distribuzione del pacchetto di installazione.
- `kmlisten.kpd`: file di descrizione dell'applicazione.

Per creare il pacchetto di installazione di Kaspersky Endpoint Security for Android:

1. Nella struttura della console selezionare la cartella **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.

2. Nell'area di lavoro della cartella **Pacchetti di installazione** fare clic sul pulsante **Crea pacchetto di installazione**.

   Verrà avviata la procedura guidata per la creazione del pacchetto di installazione. Seguire le istruzioni della procedura guidata.

3. Nella finestra **Selezionare il tipo di pacchetto di installazione** della procedura guidata fare clic sul pulsante **Crea pacchetto di installazione per un'applicazione Kaspersky**.

4. Nella finestra **Definizione del nome del pacchetto di installazione** della procedura guidata immettere il nome del pacchetto di installazione che verrà visualizzato nell'area di lavoro della cartella **Pacchetti di installazione**.

5. Nella finestra **Selezionare il pacchetto di installazione per l'installazione dell'applicazione** della procedura guidata selezionare l'archivio autoestraente `sc_package.exe` incluso nel kit di distribuzione.

   Se l'archivio è già stato decompresso, scegliere il file di descrizione dell'applicazione, `kmlisten.kpd`. Il nome dell'applicazione e il numero di versione vengono visualizzati nel campo di immissione.

6. Nella finestra **Accetta Contratto di licenza con l'utente finale** della procedura guidata leggere, comprendere e accettare i termini e le condizioni del Contratto di licenza con l'utente finale.

   È necessario accettare i termini e le condizioni del Contratto di licenza con l'utente finale per la creazione del pacchetto di installazione. Se si accettano i termini del Contratto di licenza in Administration Console, Kaspersky Endpoint Security for Android ignora il passaggio di accettazione durante l'installazione dell'app.

   Se si decide di arrestare la protezione dei dispositivi mobili, è possibile disinstallare l'app Kaspersky Endpoint Security for Android e revocare il Contratto di licenza con l'utente finale per l'app. Per ulteriori informazioni sulla revoca del Contratto di licenza con l'utente finale, fare riferimento alla *Guida di Kaspersky Security Center*.

Al termine della procedura guidata, il pacchetto di installazione creato viene visualizzato nell'area di lavoro della cartella **Pacchetti di installazione**. I pacchetti di installazione sono archiviati nella cartella Packages, nella cartella condivisa pubblica in Administration Server.

Per configurare le impostazioni del pacchetto di installazione:

1. Nella struttura della console selezionare la cartella **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.

2. Nel menu di scelta rapida per il pacchetto di installazione di Kaspersky Endpoint Security for Android selezionare **Proprietà**.

3. Nella scheda **Impostazioni** specificare le impostazioni di connessione all'Administration Server per i dispositivi mobili e il nome del gruppo di amministrazione a cui verranno aggiunti automaticamente i dispositivi mobili dopo la prima sincronizzazione con l'Administration Server. Eseguire le seguenti operazioni:

   - Nel campo **Indirizzo server** della sezione **Connessione all'Administration Server** digitare il nome dell'Administration Server per i dispositivi mobili nel formato utilizzato per l'installazione di **Supporto per dispositivi mobili** durante la distribuzione di Administration Server.

     A seconda del formato del nome dell'Administration Server per il componente **Supporto per dispositivi mobili**, specificare il nome DNS o l'indirizzo IP dell'Administration Server. Nel campo **Numero porta SSL** specificare il numero della porta nell'Administration Server aperta per le connessioni dei dispositivi mobili. Per impostazione predefinita, viene utilizzata la porta 13292.

   - Nel campo **Nome del gruppo** della sezione **Allocazione dei computer ai gruppi** digitare il nome del gruppo a cui aggiungere i dispositivi mobili dopo la prima sincronizzazione con l'Administration Server (per impostazione predefinita, viene utilizzato **KES10**).

     Il gruppo specificato verrà automaticamente creato nella cartella **Avanzate** → **Polling della rete** → **Domini**.

- Nella sezione **Azioni durante l'installazione** selezionare la casella di controllo **Richiedi indirizzo e-mail** se si desidera che l'app richieda agli utenti di fornire l'indirizzo e-mail aziendale al primo avvio dell'app.

  L'indirizzo e-mail dell'utente viene utilizzato per creare un nome per il dispositivo mobile quando questo viene aggiunto al gruppo di amministrazione.

4. Per applicare le impostazioni specificate, fare clic su **Applica**.

Creazione di un pacchetto di installazione indipendente

Per creare un pacchetto di installazione indipendente, eseguire le seguenti operazioni:

1. Nella struttura della console selezionare la cartella **Avanzate → Installazione remota → Pacchetti di installazione**.

2. Scegliere il pacchetto di installazione di Kaspersky Endpoint Security for Android.

3. Dal menu di scelta rapida del pacchetto di installazione, selezionare **Crea pacchetto di installazione indipendente**.

   Verrà avviata la procedura guidata per la creazione del pacchetto di installazione indipendente. Seguire le istruzioni della procedura guidata.

4. Configurare le modalità di distribuzione del pacchetto di installazione indipendente:

   - Per distribuire agli utenti il percorso del pacchetto di installazione indipendente tramite e-mail, nella sezione **Altre azioni** fare clic sul collegamento **Invia il collegamento al pacchetto indipendente tramite e-mail**.

     Viene visualizzata la finestra dell'editor dei messaggi e nel testo presente nella finestra è contenuto il percorso della cartella condivisa con il pacchetto di installazione indipendente.

   - Per pubblicare il collegamento al pacchetto di installazione indipendente creato nel sito Web aziendale, fare clic sul collegamento **Codice HTML di esempio per la pubblicazione del collegamento in un sito Web**.

     Viene aperto un file tmp contenente collegamenti HTML_RJL.

5. Per pubblicare il pacchetto di installazione indipendente creato nel server Web di Kaspersky Security Center e visualizzare l'intero elenco di pacchetti indipendenti per il pacchetto di installazione selezionato, nella finestra **Creazione guidata pacchetto di installazione indipendente completata** selezionare la casella **Apri l'elenco dei pacchetti indipendenti**.

Dopo la chiusura della procedura guidata, verrà visualizzata la finestra **Elenco dei pacchetti indipendenti per il pacchetto di installazione <Nome del pacchetto di installazione>**.

La finestra **Elenco dei pacchetti indipendenti per il pacchetto di installazione <Nome del pacchetto di installazione>** contiene le seguenti informazioni:

- Un elenco di pacchetti di installazione indipendenti.
- Il percorso di rete della cartella condivisa nel campo **Percorso**.
- L'indirizzo del pacchetto indipendente sul server Web di Kaspersky Security Center nel campo **URL**.

Per l'invio delle notifiche tramite e-mail, è possibile specificare l'indirizzo nel campo **URL** o il percorso nel campo **Percorso** come risorsa da cui gli utenti possono scaricare il file di installazione dell'app. Per l'invio agli utenti delle notifiche tramite messaggi di testo, è necessario specificare il collegamento di download visualizzato nel campo **URL**.

È consigliabile copiare negli Appunti l'indirizzo del pacchetto indipendente creato e quindi incollarlo nella notifica tramite e-mail o messaggio di testo per gli utenti.

Configurazione delle impostazioni di sincronizzazione

Per gestire i dispositivi mobili e ricevere rapporti o statistiche dai dispositivi mobili degli utenti, è necessario configurare le impostazioni di sincronizzazione. La sincronizzazione dei dispositivi mobili con Kaspersky Security Center può essere eseguita nei seguenti modi:

- **In base alla pianificazione**. La sincronizzazione in base alla pianificazione viene eseguita tramite il protocollo HTTP. È possibile configurare la pianificazione della sincronizzazione nelle impostazioni dei criteri di gruppo. Le modifiche apportate alle impostazioni dei criteri di gruppo, a comandi e attività verranno eseguite durante la sincronizzazione del dispositivo con Kaspersky Security Center in base alla pianificazione, e quindi con un ritardo. Per impostazione predefinita, i dispositivi mobili vengono sincronizzati automaticamente con Kaspersky Security Center ogni 6 ore.

  In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

- **Forzata**. La sincronizzazione forzata viene eseguita utilizzando le notifiche push del servizio FCM (Firebase Cloud Messaging). La sincronizzazione forzata è orientata principalmente all'invio tempestivo dei comandi a un dispositivo mobile. Se si desidera utilizzare la sincronizzazione forzata, assicurarsi che le impostazioni GSM siano configurate in Kaspersky Security Center. Per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Security Center.

Per configurare le impostazioni di sincronizzazione del dispositivo mobile con Kaspersky Security Center:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Sincronizzazione**.
5. Selezionare la frequenza di sincronizzazione nell'elenco a discesa **Sincronizza**.
6. Per disabilitare la sincronizzazione di un dispositivo con Kaspersky Security Center durante il roaming, selezionare la casella **Non sincronizzare in roaming**.

   L'utente del dispositivo può eseguire manualmente la sincronizzazione nelle impostazioni dell'app (→ **Impostazioni** → **Sincronizzazione** → **Sincronizza**).
7. Per nascondere all'utente le impostazioni di sincronizzazione (indirizzo del server, porta e gruppo di amministrazione) nelle impostazioni dell'app, deselezionare la casella **Mostra impostazioni di sincronizzazione nel dispositivo**. È impossibile modificare le impostazioni nascoste.
8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. È possibile sincronizzare manualmente il dispositivo mobile utilizzando un comando specifico. Per sapere di più su come utilizzare i comandi per dispositivi mobili, fare riferimento alla *Guida di Kaspersky Security Center*.

Attivazione dell'app Kaspersky Endpoint Security for Android

In Kaspersky Security Center, la licenza può coprire vari gruppi di funzionalità. Per garantire la piena operatività dell'app Kaspersky Endpoint Security for Android, la licenza di Kaspersky Security Center acquistata dall'organizzazione deve offrire la funzionalità **Mobile Device Management**. La funzionalità **Mobile Device Management** è progettata per la connessione dei dispositivi mobili a Kaspersky Security Center e per la relativa gestione.

Per informazioni dettagliate sulle licenze di Kaspersky Security Center e sulle opzioni di licenza, fare riferimento alla *Guida di Kaspersky Security Center*.

L'attivazione dell'app Kaspersky Endpoint Security for Android in un dispositivo mobile viene eseguita fornendo all'app informazioni di licenza valide. Le informazioni sulla licenza vengono distribuite al dispositivo mobile insieme al criterio quando il dispositivo viene sincronizzato con Kaspersky Security Center.

Se l'attivazione dell'app Kaspersky Endpoint Security for Android non viene completata entro 30 giorni dal momento dell'installazione nel dispositivo mobile, l'app passerà automaticamente alla modalità con funzionalità limitate. In questa modalità, la maggior parte dei componenti dell'app non è operativa. Quando passa alla modalità con funzionalità limitate, l'app smette di eseguire la sincronizzazione automatica con Kaspersky Security Center. Pertanto, se l'attivazione dell'app non viene completata entro 30 giorni dall'installazione, l'utente deve sincronizzare manualmente il dispositivo con Kaspersky Security Center.

Se Kaspersky Security Center non è distribuito nell'organizzazione o non è accessibile ai dispositivi mobili, gli utenti possono attivare manualmente l'app Kaspersky Endpoint Security for Android nei propri dispositivi.

Per attivare l'app Kaspersky Endpoint Security for Android:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Licenza**.
5. Nella sezione **Licensing** aprire l'elenco a discesa **Chiave**, quindi selezionare la chiave di attivazione dell'applicazione desiderata nell'archivio delle chiavi di Kaspersky Security Center Administration Server.

   Nel campo sottostante sono visualizzati i dettagli dell'app per cui è stata acquistata la licenza.
6. Selezionare la casella **Attiva con una chiave dall'archivio di Kaspersky Security Center**.

   Se l'app è stata attivata senza un codice memorizzato nell'archivio di Kaspersky Security Center, Kaspersky Security for Mobile sostituisce questo codice con il codice di attivazione selezionato nell'elenco a discesa **Codice**.
7. Per attivare l'app nel dispositivo mobile dell'utente, bloccare le modifiche alle impostazioni.
8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Installazione di un profilo MDM iOS

Questa sezione descrive i metodi di distribuzione dei profili MDM iOS in una rete aziendale.

Prima di distribuire un profilo MDM iOS, l'amministratore deve eseguire le seguenti operazioni:

1. Installare un server MDM iOS.
2. Ottenere un certificato APN (Apple Push Notification).
3. Installare un certificato APN nel server MDM iOS.

Per maggiori dettagli sull'installazione di un server MDM iOS e sull'utilizzo di un certificato APNs, fare riferimento alla *Guida di Kaspersky Security Center*.

Per informazioni dettagliate sulla distribuzione di un profilo MDM iOS in Kaspersky Endpoint Security Cloud, fare riferimento alla *Guida di Kaspersky Endpoint Security Cloud*.

Informazioni sulle modalità di gestione dei dispositivi iOS

È possibile distribuire un sistema di gestione dei dispositivi iOS in vari modi. La modalità di gestione dipende dal proprietario del dispositivo mobile (personale o aziendale) e dai requisiti di sicurezza aziendali. È possibile selezionare la modalità di gestione più adatta per l'azienda e utilizzare diverse modalità contemporaneamente.

Dispositivi non supervisionati

I *dispositivi iOS non supervisionati* sono i dispositivi personali dei dipendenti che sono connessi a Kaspersky Security Center. In questa modalità, l'utente è autorizzato a utilizzare un ID Apple personale, lavorare con qualsiasi app e archiviare dati personali nel dispositivo. È possibile utilizzare un criterio di gruppo di Kaspersky Device Management for iOS per configurare l'accesso a risorse aziendali, impostazioni di sicurezza e altre impostazioni. Per impostazione predefinita, tutti i dispositivi iOS non sono supervisionati.

Dispositivi supervisionati

I *dispositivi iOS supervisionati* sono i dispositivi aziendali che sono connessi a Kaspersky Security Center. La configurazione iniziale del dispositivo mobile viene eseguita in Apple Configurator. *Apple Configurator* è un'applicazione progettata per preparare e configurare i dispositivi iOS. Apple Configurator è installato in un computer che esegue OS X. Per maggiori informazioni sull'utilizzo di Apple Configurator, fare riferimento al sito Web dell'assistenza tecnica Apple. È possibile utilizzare un criterio di gruppo di Kaspersky Device Management for iOS per un'ulteriore configurazione. Nei dispositivi supervisionati, è possibile accedere a una selezione estesa di impostazioni. È ad esempio possibile configurare il proxy HTTP globale e restrizioni aggiuntive (ad esempio, blocco dell'utilizzo di iMessage e Game Center), nonché bloccare le modifiche dell'account utente.

Per utilizzare i dispositivi iOS supervisionati e non supervisionati, il server MDM iOS deve disporre di un certificato APN installato e un profilo MDM iOS deve essere installato nei dispositivi mobili degli utenti.

Installazione tramite Kaspersky Security Center

Il profilo MDM iOS viene installato nei dispositivi mobili degli utenti i cui account utente sono stati aggiunti in Kaspersky Security Center. Per maggiori informazioni sugli account utente in Kaspersky Security Center, fare riferimento alla *Guida di Kaspersky Security Center*.

Per installare un profilo MDM iOS:

1. Nella struttura della console selezionare la cartella **Mobile Device Management** → **Dispositivi mobili**.
2. Nell'area di lavoro della cartella **Dispositivi mobili** fare clic sul pulsante **Aggiungi dispositivo mobile**.

   Verrà avviata la procedura guidata per la connessione di un nuovo dispositivo mobile. Seguire le istruzioni della procedura guidata.
3. Nella finestra **Sistema operativo** della procedura guidata selezionare **iOS**.
4. Nella finestra **Metodo di protezione dei dispositivi MDM iOS** della procedura guidata selezionare **Usa il profilo MDM iOS del server MDM iOS** e specificare il profilo MDM iOS nell'elenco.
5. Nella finestra **Seleziona utenti** della procedura guidata selezionare uno o più utenti per l'installazione del profilo MDM iOS nei relativi dispositivi mobili.

   Se l'utente non è nell'elenco, è possibile aggiungere un nuovo account utente senza uscire dalla procedura guidata per la connessione di un nuovo dispositivo mobile.
6. Nella finestra **Origine certificato** della procedura guidata selezionare l'origine del certificato per la protezione del trasferimento dei dati tra il dispositivo mobile e Kaspersky Security Center:

   - **Rilasciare il certificato attraverso gli strumenti di Administration Server**. In questo caso, il certificato verrà creato automaticamente.
   - **Specificare il file di certificato**. In questo caso, il certificato deve essere preparato per tempo ed essere successivamente selezionato nella finestra della procedura guidata. Questa opzione non può essere utilizzata se si desidera installare il profilo MDM iOS in più dispositivi mobili. È necessario creare un certificato distinto per ogni utente.
7. Nella finestra **Metodo di notifica all'utente** della procedura guidata selezionare il canale utilizzato per inoltrare il collegamento per l'installazione dell'app:

   - Per inviare il collegamento tramite e-mail, selezionare **Invia collegamento al profilo MDM iOS** e configurare le impostazioni nella sezione **Tramite e-mail**. Accertarsi che l'indirizzo e-mail sia specificato nelle impostazioni degli account utente.
   - Per inviare il collegamento tramite messaggio SMS, selezionare **Invia collegamento al profilo MDM iOS** e configurare le impostazioni nella sezione **Tramite SMS**. Accertarsi che il numero di telefono sia specificato nelle impostazioni degli account utente.
   - Per installare il profilo MDM iOS utilizzando un codice QR, selezionare **Mostra collegamento al pacchetto di installazione** ed esaminare il codice QR utilizzando la fotocamera del dispositivo mobile.
   - Se nessuno dei metodi elencati è idoneo, selezionare **Mostra collegamento al pacchetto di installazione** → **Copia** per copiare il collegamento per l'installazione del profilo MDM iOS negli Appunti. Utilizzare qualsiasi metodo disponibile per inviare il collegamento per l'installazione dell'app.
8. Terminare la procedura guidata per la connessione di un nuovo dispositivo mobile.

Dopo l'installazione del profilo MDM iOS nei dispositivi mobili degli utenti, sarà possibile configurare le impostazioni dell'app utilizzando i criteri di gruppo. Sarà inoltre possibile inviare comandi ai dispositivi mobili per la protezione dei dati in caso di furto o smarrimento dei dispositivi.

Nei dispositivi mobili che eseguono iOS 12.1 o versioni successive è necessario confermare manualmente l'installazione di un profilo MDM iOS nel dispositivo mobile. È inoltre necessario concedere l'autorizzazione per la gestione remota del dispositivo.

Installazione dei plug-in di amministrazione

Per gestire i dispositivi mobili, nella workstation dell'amministratore devono essere installati i plug-in di amministrazione seguenti:

- Il plug-in di amministrazione di Kaspersky Endpoint Security for Android fornisce l'interfaccia per la gestione dei dispositivi mobili e delle app mobili installate in essi tramite Administration Console di Kaspersky Security Center.
- Il plug-in di amministrazione di Kaspersky Device Management for iOS fornisce un'interfaccia per gestire i dispositivi mobili connessi tramite il protocollo Exchange ActiveSync e MDM iOS mediante Administration Console di Kaspersky Security Center.

È possibile installare i plug-in di amministrazione utilizzando i seguenti metodi:

- Installare un plug-in di amministrazione utilizzando l'Avvio rapido guidato di Kaspersky Security Center.

  L'applicazione richiede automaticamente di eseguire l'Avvio rapido guidato dopo l'installazione di Administration Server, alla prima connessione. È inoltre possibile avviare manualmente l'Avvio rapido guidato in qualsiasi momento.

  L'Avvio rapido guidato consente di accettare i termini e le condizioni del Contratto di Licenza con l'utente finale per Kaspersky Endpoint Security per l'app Android in Administration Console. Se l'amministratore accetta i termini del Contratto di licenza in Administration Console, Kaspersky Endpoint Security for Android ignora il passaggio di accettazione durante l'installazione dell'app. Per ulteriori dettagli sull'Avvio rapido guidato per Kaspersky Security Center, fare riferimento alla *Guida di Kaspersky Security Center*.

- Installare il plug-in di amministrazione utilizzando l'elenco dei pacchetti di distribuzione disponibili in Administration Console di Kaspersky Security Center.

  L'elenco dei pacchetti di distribuzione disponibili viene aggiornato automaticamente dopo il rilascio di nuove versioni delle applicazioni Kaspersky.

- Scaricare il pacchetto di distribuzione da un'origine esterna e installare il plug-in di amministrazione utilizzando il file EXE.

  Il pacchetto di distribuzione del plug-in di amministrazione può ad esempio essere scaricato sul sito Web Kaspersky.

Installazione dei plug-in di amministrazione dall'elenco in Administration Console

Per installare i plug-in di amministrazione:

1. Nella struttura della console selezionare **Avanzate** → **Installazione remota** → **Pacchetti di installazione**.

2. Nell'area di lavoro selezionare **Azioni aggiuntive** → **Visualizza le versioni correnti delle applicazioni Kaspersky**.

   Si aprirà l'elenco delle versioni aggiornate delle applicazioni Kaspersky.

3. Nella sezione **Dispositivi mobili** selezionare il plug-in **Kaspersky Endpoint Security for Android** o **Kaspersky Device Management for iOS**.

4. Fare clic sul pulsante **Scarica pacchetti di distribuzione**.

   Un file di distribuzione del plug-in verrà scaricato nella memoria del computer (file EXE).

5. Eseguire il file EXE e seguire le istruzioni dell'Installazione guidata.

Installazione dei plug-in di amministrazione dal pacchetto di distribuzione

Per installare il plug-in di amministrazione di Kaspersky Endpoint Security for Android,

copiare il file di installazione del plug-in `klcfinst.exe` dal pacchetto di distribuzione della soluzione integrata ed eseguirlo nella workstation di amministrazione.

L'installazione viene eseguita dalla procedura guidata e non è necessario configurare le impostazioni.

Per installare il plug-in di amministrazione di Kaspersky Device Management for iOS,

copiare il file di installazione del plug-in `klmdminst.exe` dal pacchetto di distribuzione della soluzione integrata ed eseguirlo nella workstation di amministrazione.

L'installazione viene eseguita dalla procedura guidata e non è necessario configurare le impostazioni.

È possibile verificare che i plug-in di amministrazione siano installati visualizzando l'elenco dei plug-in di amministrazione delle app installati nella finestra delle proprietà di Administration Server nella sezione **Avanzate** → **Dettagli dei plug-in di gestione applicazioni installati**.

Aggiornamento di una versione precedente dell'applicazione

L'upgrade dell'applicazione deve soddisfare i seguenti requisiti:

- La versione del plug-in di amministrazione di Kaspersky Endpoint Security e la versione dell'app mobile Kaspersky Endpoint Security for Android devono corrispondere.

  È possibile visualizzare i numeri delle build delle versioni del plug-in di amministrazione e dell'app mobile nelle note sulla versione relative a Kaspersky Security for Mobile.

- Accertarsi che Kaspersky Security Center soddisfi i requisiti software di Kaspersky Security for Mobile.

- È possibile eseguire automaticamente l'upgrade dei plug-in di amministrazione di Kaspersky Endpoint Security 10.0 Service Pack 2 (build 10.6.0.1801) e Kaspersky Device Management for iOS 10.0 Service Pack 2 (build 10.6.0.1767) e versioni successive alla versione corrente. Gli upgrade delle versioni precedenti dei plug-in di amministrazione non sono supportati.

  Per eseguire l'upgrade dei plug-in di amministrazione delle versioni precedenti, è necessario rimuovere i plug-in di amministrazione installati e i criteri di gruppo creati contestualmente. Installare quindi le nuove versioni dei plug-in di amministrazione. Per informazioni dettagliate sulla rimozione dei plug-in di amministrazione, visitare il *sito Web dell'Assistenza tecnica di Kaspersky*.

- Utilizzare la stessa versione di Kaspersky Endpoint Security for Android in tutti i dispositivi mobili dell'organizzazione.

I termini e le condizioni dell'assistenza tecnica per le versioni di Kaspersky Security for Mobile sono disponibili nel *sito Web dell'Assistenza tecnica di Kaspersky*.

Per visualizzare la versione e il numero di build dei plug-in di amministrazione:

1. Nella struttura della console nel menu di scelta rapida di Administration Server selezionare **Proprietà**.
2. Nella finestra delle proprietà di Administration Server selezionare **Avanzate** → **Dettagli dei plug-in di gestione applicazioni installati**.

   L'area di lavoro visualizza informazioni sui plug-in di amministrazione installati nel formato `<Nome plug-in> <Versione> <Build>`.

È possibile visualizzare la versione e il numero di build dell'app di Kaspersky Endpoint Security for Android utilizzando i seguenti metodi:

- Se Kaspersky Endpoint Security for Android è stato installato con un pacchetto di installazione indipendente, è possibile visualizzare la versione e il numero di build dell'app nelle proprietà del pacchetto.
- Se Kaspersky Endpoint Security for Android è stato installato tramite Google Play, è possibile visualizzare il numero di build nelle impostazioni dell'app (→ **Informazioni sull'app**).

Upgrade della versione precedente di Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android può essere aggiornato nei seguenti modi:

- Utilizzando Google Play. L'utente del dispositivo mobile scarica la nuova versione dell'app da Google Play e la installa nel dispositivo.
- Utilizzando Kaspersky Security Center. È possibile aggiornare in remoto la versione dell'app nel dispositivo utilizzando il sistema di amministrazione remota Kaspersky Security Center.

È possibile selezionare il metodo di aggiornamento dell'app più adatto all'organizzazione. È possibile utilizzare un solo metodo di aggiornamento.

Aggiornamento dell'app da Google Play

L'app può essere aggiornata da Google Play seguendo la procedura di aggiornamento standard della piattaforma Android. Per l'aggiornamento dell'app devono essere soddisfatte le seguenti condizioni:

- L'utente del dispositivo deve avere un account Google.
- Il dispositivo deve essere associato all'account Google.
- Il dispositivo deve essere connesso a Internet.

Dopo il download dell'app da Google Play, Kaspersky Endpoint Security for Android verifica i termini e le condizioni del Contratto di Licenza con l'utente finale (EULA). Se i termini del Contratto di licenza con l'utente finale sono aggiornati, l'app invia una richiesta a Kaspersky Security Center. Se l'amministratore accetta il Contratto di licenza con l'utente finale in Administration Console, Kaspersky Endpoint Security for Android ignora il passaggio di accettazione durante l'installazione dell'app. Se l'amministratore utilizza una versione obsoleta del plug-in di amministrazione, Kaspersky Security Center richiede di aggiornare il plug-in di amministrazione. Durante l'aggiornamento del plug-in di amministrazione, un amministratore può accettare le condizioni del Contratto di licenza con l'utente finale in Administration Console per Kaspersky Endpoint Security for Android.

È possibile eseguire l'aggiornamento dell'app tramite Google Play se Kaspersky Endpoint Security for Android è stato installato da Google Play. Se l'app è stata installata con un altro metodo, non è possibile eseguire l'aggiornamento dell'app tramite Google Play.

Aggiornamento dell'app tramite Kaspersky Security Center

L'upgrade di Kaspersky Endpoint Security for Android può essere eseguito utilizzando Kaspersky Security Center in seguito all'applicazione di un criterio di gruppo. Nelle impostazioni del criterio di gruppo è possibile selezionare la versione del pacchetto di installazione indipendente di Kaspersky Endpoint Security for Android che soddisfa i requisiti di sicurezza aziendali.

È possibile eseguire l'aggiornamento tramite Kaspersky Security Center se Kaspersky Endpoint Security for Android è stato installato tramite Kaspersky Security Center. Se l'app è stata installata da Google Play, non è possibile aggiornare l'app tramite Kaspersky Security Center.

Per eseguire l'upgrade di Kaspersky Endpoint Security for Android utilizzando un pacchetto di installazione indipendente, l'installazione delle app da origini sconosciute deve essere consentita nel dispositivo mobile dell'utente. Per ulteriori informazioni sull'installazione delle app senza Google Play, fare riferimento alla *Guida Android*.

Per aggiornare la versione dell'app:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Avanzate**.
5. Nella sezione **Upgrade di Kaspersky Endpoint Security for Android** fare clic sul pulsante **Seleziona**.

   Verrà visualizzata la finestra **Upgrade di Kaspersky Endpoint Security for Android**.
6. Nell'elenco dei pacchetti di installazione indipendenti di Kaspersky Endpoint Security selezionare il pacchetto la cui versione soddisfa i requisiti di sicurezza aziendali.

   È possibile aggiornare Kaspersky Endpoint Security solo a una versione più recente dell'applicazione. Kaspersky Endpoint Security non può essere aggiornato a una versione precedente dell'applicazione.
7. Fare clic sul pulsante **Seleziona**.

Viene visualizzata una descrizione del pacchetto di installazione indipendente selezionato nella sezione **Upgrade di Kaspersky Endpoint Security for Android**.

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. All'utente del dispositivo mobile viene richiesto di installare la nuova versione dell'app. Se l'utente acconsente, la nuova versione dell'app viene installata nel dispositivo mobile.

Installazione di una versione precedente di Kaspersky Endpoint Security for Android

Se si desidera impedire l'aggiornamento automatico dell'app e utilizzare una versione specifica di Kaspersky Endpoint Security for Android, disabilitare l'aggiornamento automatico dell'app nelle impostazioni di Google Play. Per maggiori dettagli, consultare il sito Web dell'assistenza tecnica Google.

L'aggiornamento automatico di Kaspersky Endpoint Security for Android è disponibile solo se l'app è stata installata da Google Play o tramite Kaspersky Security Center utilizzando il collegamento di Google Play. Se l'app è stata installata tramite Kaspersky Security Center utilizzando un collegamento al proprio server Web (con il pacchetto di installazione indipendente), l'aggiornamento automatico non è disponibile. In questo caso è possibile utilizzare un criterio di gruppo per aggiornare manualmente Kaspersky Endpoint Security for Android.

Per installare una versione precedente di Kaspersky Endpoint Security for Android:

1. Rimuovere Kaspersky Endpoint Security for Android dai dispositivi mobili degli utenti.

2. Installare Kaspersky Endpoint Security for Android tramite Kaspersky Security Center utilizzando un collegamento al proprio server Web. A tale scopo, è necessario il pacchetto di installazione per la versione specifica. È possibile scaricare il pacchetto di distribuzione per le versioni precedenti di Kaspersky Endpoint Security for Android nel sito Web dell'Assistenza tecnica di Kaspersky.

Per informazioni dettagliate sulle versioni precedenti di Kaspersky Endpoint Security for Android, consultare la *Guida per la versione appropriata di Kaspersky Security for Mobile*.

Upgrade di versioni precedenti dei plug-in di amministrazione

È possibile eseguire l'upgrade dei plug-in di amministrazione utilizzando i seguenti metodi:

- Installare il plug-in di amministrazione della nuova versione dall'elenco dei pacchetti di distribuzione disponibili in Administration Console di Kaspersky Security Center.

  L'elenco dei pacchetti di distribuzione disponibili viene aggiornato automaticamente dopo il rilascio di nuove versioni delle applicazioni Kaspersky.

- Scaricare il pacchetto di distribuzione da un'origine esterna e installare il plug-in di amministrazione della nuova versione utilizzando il file EXE.

  Per aggiornare i plug-in di amministrazione di Kaspersky Endpoint Security for Android e Kaspersky Device Management for iOS, è necessario scaricare la versione più recente dell'applicazione dalla pagina Web di Kaspersky Security for Mobile ed eseguire l'Installazione guidata di ognuno dei due plug-in. Le versioni precedenti dei plug-in vengono rimosse automaticamente durante l'esecuzione dell'Installazione guidata.

Gli esperti di Kaspersky consigliano di utilizzare la stessa versione dell'app e dei plug-in di amministrazione. Se l'utente esegue l'upgrade dell'app da Google Play, Kaspersky Security Center mostra una notifica con la richiesta di eseguire l'upgrade del plug-in di amministrazione.

Durante l'aggiornamento dei plug-in di amministrazione, i gruppi di amministrazione esistenti nella cartella **Dispositivi gestiti** e le regole per l'assegnazione automatica a questi gruppi dei dispositivi dalla cartella **Dispositivi non assegnati** vengono salvati. Vengono inoltre salvati i criteri di gruppo esistenti per i dispositivi mobili. Le nuove impostazioni dei criteri che implementano le nuove funzioni della soluzione integrata Kaspersky Security for Mobile verranno aggiunte ai criteri esistenti con i valori predefiniti.

Se sono state aggiunte nuove impostazioni o sono stati modificati i valori predefiniti nella nuova versione del plug-in di amministrazione, le modifiche saranno applicate solo dopo l'apertura di un criterio di gruppo. Finché l'amministratore non apre un criterio di gruppo, nei dispositivi mobili saranno applicate le impostazioni della versione precedente del plug-in, anche se la versione del plug-in è stata aggiornata.

Upgrade dall'elenco in Administration Console

Per eseguire l'upgrade dei plug-in di amministrazione:

1. Nella struttura della console selezionare **Avanzate → Installazione remota → Pacchetti di installazione**.
2. Nell'area di lavoro selezionare **Azioni aggiuntive → Visualizza le versioni correnti delle applicazioni Kaspersky**.

   Si aprirà l'elenco delle versioni aggiornate delle applicazioni Kaspersky.
3. Nella sezione **Dispositivi mobili** selezionare il plug-in **Kaspersky Endpoint Security for Android** o **Kaspersky Device Management for iOS**.
4. Fare clic sul pulsante **Scarica pacchetti di distribuzione**.

   Un file di distribuzione del plug-in verrà scaricato nella memoria del computer (file EXE). Eseguire il file EXE. Seguire le istruzioni dell'Installazione guidata.

Upgrade dal pacchetto di distribuzione

Per eseguire l'upgrade del plug-in di amministrazione di Kaspersky Endpoint Security for Android,

copiare il file di installazione del plug-in `klcfinst.exe` dal pacchetto di distribuzione della soluzione integrata ed eseguirlo nella workstation di amministrazione.

L'installazione viene eseguita dalla procedura guidata e non è necessario configurare le impostazioni.

Per eseguire l'upgrade del plug-in di amministrazione di Kaspersky Device Management for iOS,

copiare il file di installazione del plug-in `klmdminst.exe` dal pacchetto di distribuzione della soluzione integrata ed eseguirlo nella workstation di amministrazione.

L'installazione del plug-in viene eseguita dalla procedura guidata e non è necessario configurare le impostazioni.

È possibile verificare che l'upgrade dei plug-in di amministrazione sia stato eseguito visualizzando l'elenco dei plug-in di amministrazione delle app installati nella finestra delle proprietà di Administration Server nella sezione **Avanzate → Dettagli dei plug-in di gestione applicazioni installati**.

Rimozione di Kaspersky Endpoint Security for Android

Kaspersky Endpoint Security for Android può essere rimosso nei seguenti modi:

1. Rimozione dell'app da parte dell'utente

   L'utente rimuove Kaspersky Endpoint Security for Android manualmente utilizzando l'interfaccia dell'app. Per consentire agli utenti di rimuovere l'app, la rimozione dell'app deve essere consentita nel criterio applicato al dispositivo.

2. Rimozione dell'app da parte dell'amministratore

   L'amministratore rimuove l'app in remoto utilizzando Administration Console di Kaspersky Security Center. L'app può essere rimossa da un singolo dispositivo o da più dispositivi contemporaneamente.

Rimozione remota dell'app

È possibile rimuovere Kaspersky Endpoint Security for Android dai dispositivi mobili degli utenti in remoto nei seguenti modi:

- Utilizzando un criterio di gruppo. Questo metodo è particolarmente utile per rimuovere l'app da più dispositivi contemporaneamente.
- Configurando le impostazioni locali dell'app. Questo metodo è particolarmente utile per rimuovere l'app da un singolo dispositivo.

Per rimuovere l'app applicando un criterio di gruppo:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Avanzate**.
5. Nella sezione **Disinstallare l'app Kaspersky Endpoint Security for Android** selezionare la casella **Disinstalla Kaspersky Endpoint Security for Android dal dispositivo**.
6. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

   Kaspersky Endpoint Security for Android viene quindi rimosso dai dispositivi mobili in seguito alla sincronizzazione con Administration Server. Gli utenti dei dispositivi mobili ricevono una notifica di rimozione dell'app.

Per rimuovere l'app configurando le impostazioni locali:

1. Nella struttura della console selezionare **Mobile Device Management → Dispositivi mobili**.

2. Nell'elenco dei dispositivi selezionare il dispositivo da cui rimuovere l'app.

3. Aprire la finestra delle proprietà del dispositivo facendo doppio clic.

4. Selezionare **App** → **Kaspersky Endpoint Security for Android**.

5. Aprire la finestra delle proprietà di Kaspersky Endpoint Security facendo doppio clic.

6. Selezionare la sezione **Avanzate**.

7. Nella sezione **Rimozione di Kaspersky Endpoint Security for Android** selezionare la casella di controllo **Disinstalla Kaspersky Endpoint Security for Android dal dispositivo**.

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Kaspersky Endpoint Security for Android viene quindi rimosso dal dispositivo mobile in seguito alla sincronizzazione con Administration Server. L'utente del dispositivo mobile riceve una notifica di rimozione dell'app.

Autorizzazione della rimozione dell'applicazione da parte degli utenti

Per proteggere l'app dalla rimozione nei dispositivi che eseguono Android 7.0 o versioni successive, Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Durante l'esecuzione della procedura guidata di configurazione iniziale, Kaspersky Endpoint Security for Android richiede all'utente di concedere all'applicazione tutte le autorizzazioni richieste. L'utente può ignorare questi passaggi o disabilitare tali autorizzazioni nelle impostazioni del dispositivo in un momento successivo. In tal caso, l'app non è protetta dalla rimozione.

È possibile consentire agli utenti di rimuovere Kaspersky Endpoint Security for Android dai propri dispositivi mobili nei seguenti modi:

- Utilizzando un criterio di gruppo. Questo metodo è particolarmente utile per consentire agli utenti di rimuovere l'app da più dispositivi contemporaneamente.

- Utilizzo delle impostazioni locali dell'app. Questo metodo è particolarmente utile per consentire all'utente di un singolo dispositivo di rimuovere l'app.

Per consentire la rimozione dell'app in un criterio di gruppo:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Avanzate**.

5. Nella sezione **Rimozione di Kaspersky Endpoint Security for Android** impostare la casella **Consenti la rimozione di Kaspersky Endpoint Security for Android**.

6. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Di conseguenza, la rimozione dell'app da parte degli utenti è consentita nei dispositivi mobili dopo la sincronizzazione con Administration Server. Il pulsante di rimozione dell'app diventa disponibile nelle impostazioni di Kaspersky Endpoint Security for Android.

Per consentire la rimozione dell'app nelle impostazioni locali dell'app:

1. Nella struttura della console selezionare **Avanzate** → **Mobile Device Management** → **Dispositivi mobili**.
2. Nell'elenco dei dispositivi selezionare il dispositivo per cui consentire la rimozione dell'app da parte dell'utente.
3. Aprire la finestra delle proprietà del dispositivo facendo doppio clic.
4. Selezionare **Applicazioni** → **Kaspersky Endpoint Security for Mobile**.
5. Aprire la finestra delle proprietà di Kaspersky Endpoint Security facendo doppio clic.
6. Selezionare la sezione **Avanzate**.
7. Nella sezione **Rimozione di Kaspersky Endpoint Security for Android** impostare la casella **Consenti la rimozione di Kaspersky Endpoint Security for Android**.
8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Di conseguenza, la rimozione dell'app da parte dell'utente è consentita nel dispositivo mobile dopo la sincronizzazione con Administration Server. Il pulsante di rimozione dell'app diventa disponibile nelle impostazioni di Kaspersky Endpoint Security for Android.

Rimozione dell'app da parte dell'utente

Per rimuovere autonomamente Kaspersky Endpoint Security for Android da un dispositivo mobile, l'utente deve procedere come segue:

1. Nella finestra principale di Kaspersky Endpoint Security for Android toccare → **Disinstalla app**.

   Viene visualizzata una richiesta di conferma sullo schermo.

   Se il pulsante **Disinstalla app** non è disponibile, l'amministratore ha abilitato la protezione dalla rimozione di Kaspersky Endpoint Security for Android.
2. Confermare la rimozione di Kaspersky Endpoint Security for Android.

L'app di Kaspersky Endpoint Security for Android verrà rimossa dal dispositivo mobile dell'utente.

Configurazione e gestione

Questa sezione della Guida è destinata agli specialisti che amministrano Kaspersky Security for Mobile, nonché agli specialisti che forniscono assistenza tecnica alle organizzazioni che utilizzano Kaspersky Security for Mobile.

Introduzione

Questa sezione descrive le azioni che è consigliabile eseguire per iniziare a usare Kaspersky Security for Mobile.

Avvio e arresto dell'applicazione

Kaspersky Security Center avvia e arresta automaticamente i plug-in di amministrazione di Kaspersky Endpoint Security e Kaspersky Device Management for iOS.

Kaspersky Endpoint Security for Android viene avviato all'avvio del sistema operativo e protegge il dispositivo mobile durante l'intera sessione. L'utente può arrestare l'app disabilitando tutti i componenti di Kaspersky Endpoint Security for Android. È possibile utilizzare i criteri di gruppo per configurare le autorizzazioni utente per la gestione dei componenti dell'app.

In determinati dispositivi (ad esempio Huawei, Meizu e Xiaomi), è necessario aggiungere manualmente Kaspersky Endpoint Security for Android all'elenco delle app eseguite all'avvio del sistema operativo (**Sicurezza** → **Autorizzazioni** → **Esecuzione automatica**). Se l'app non viene aggiunta all'elenco, Kaspersky Endpoint Security for Android interrompe l'esecuzione di tutte le funzioni in seguito al riavvio del dispositivo mobile.

È inoltre necessario disabilitare la modalità Risparmio batteria per Kaspersky Endpoint Security for Android. Questa operazione è richiesta per consentire l'esecuzione dell'app in background, ad esempio per l'esecuzione di una scansione virus pianificata o la sincronizzazione del dispositivo con Kaspersky Security Center. Questo problema è attribuibile alle specifiche funzionalità del software incorporato in tali dispositivi.

Creazione di un gruppo di amministrazione

Per eseguire la configurazione centralizzata dell'app Kaspersky Endpoint Security for Android installata nei dispositivi mobili degli utenti, è necessario applicare i criteri di gruppo ai dispositivi.

Per applicare il criterio a un gruppo di dispositivi, è consigliabile creare un gruppo distinto per tali dispositivi in **Dispositivi gestiti** prima di installare le app mobili nei dispositivi degli utenti.

Dopo la creazione di un gruppo di amministrazione, è consigliabile configurare l'opzione per l'assegnazione automatica dei dispositivi in cui si desidera installare le app a questo gruppo. Configurare quindi le impostazioni comuni a tutti i dispositivi utilizzando un criterio di gruppo.

Per creare un gruppo di amministrazione, eseguire le seguenti operazioni:

1. Nella struttura della console aprire la cartella **Dispositivi gestiti**.
2. Nell'area di lavoro della cartella o sottocartella **Dispositivi gestiti** selezionare la scheda **Dispositivi**.
3. Fare clic sul pulsante **Nuovo gruppo**.

   Verrà visualizzata la finestra in cui è possibile creare un nuovo gruppo.
4. Nella finestra **Nome del gruppo** digitare il nome del gruppo e fare clic su **OK**.

Una nuova cartella per il gruppo di amministrazione con il nome specificato verrà visualizzata nella struttura della console. Per informazioni dettagliate sull'utilizzo dei gruppi di amministrazione, vedere la *Guida di Kaspersky Security Center*.

Criteri di gruppo per la gestione dei dispositivi mobili

Un *criterio di gruppo* è un pacchetto di impostazioni per la gestione dei dispositivi mobili che appartengono a un gruppo di amministrazione e delle app mobili installate nei dispositivi. È possibile creare un criterio di gruppo tramite la Creazione guidata nuovo criterio.

È possibile utilizzare un criterio per configurare le impostazioni sia di singoli dispositivi che di un gruppo di dispositivi. Per un gruppo di dispositivi, le impostazioni di amministrazione possono essere configurate nella finestra delle proprietà del criterio di gruppo. Per un singolo dispositivo, possono essere configurate nella finestra delle impostazioni locali dell'applicazione. Le singole impostazioni di gestione specificate per un dispositivo possono essere diverse dai valori delle impostazioni configurate nel criterio per un gruppo a cui appartiene il dispositivo.

Ogni parametro rappresentato in un criterio dispone di un attributo di "blocco", che indica se è consentita la modifica dell'impostazione nei criteri dei livelli nidificati della gerarchia (per i gruppi nidificati e gli Administration Server secondari) nelle impostazioni locali dell'applicazione.

I valori delle impostazioni configurate nel criterio e nelle impostazioni locali dell'applicazione vengono salvati nell'Administration Server, distribuite ai dispositivi mobili durante la sincronizzazione e salvate nei dispositivi come impostazioni correnti. Se l'utente ha specificato altri valori delle impostazioni che non sono stati "bloccati", durante la successiva sincronizzazione del dispositivo con l'Administration Server i nuovi valori delle impostazioni vengono inviati all'Administration Server e salvati nelle impostazioni locali dell'applicazione invece dei valori specificati in precedenza dall'amministratore.

Per tenere aggiornata la protezione aziendale dei dispositivi mobili, è possibile monitorare la conformità dei dispositivi degli utenti con il criterio di gestione di gruppo.

L'indicatore del livello di protezione è visualizzato nella parte superiore della finestra dei criteri di gruppo. L'indicatore del livello di protezione consente di configurare il criterio in modo da garantire un livello elevato di protezione del dispositivo. Lo stato dell'indicatore del livello di protezione cambia in base alle impostazioni del criterio:

- **Livello di protezione alto**: viene garantito un livello appropriato di protezione del dispositivo. Tutti i componenti di protezione funzionano in base alle impostazioni consigliate da Kaspersky.
- **Livello di protezione medio**: il livello di protezione è più basso di quello consigliato. Alcuni componenti della protezione critici sono disabilitati (ad esempio Protezione Web). I problemi importanti sono contrassegnati con l'icona .
- **Livello di protezione basso**: sono presenti problemi che possono causare l'infezione del dispositivo e la perdita dei dati. Alcuni componenti della protezione critici sono disabilitati (ad esempio la protezione in tempo reale dei dispositivi è disabilitata). I problemi critici sono contrassegnati con l'icona .

Per ulteriori informazioni sulla gestione dei criteri e dei gruppi di amministrazione in Administration Console di Kaspersky Security Center, vedere la *Guida di Kaspersky Security Center*.

Creazione di un criterio di gruppo

Questa sezione descrive il processo di creazione dei criteri di gruppo per i dispositivi in cui è installata l'app mobile Kaspersky Endpoint Security for Android e i criteri per i dispositivi EAS e MDM iOS.

I criteri creati per un gruppo di amministrazione sono visualizzati nell'area di lavoro del gruppo in Administration Console di Kaspersky Security Center, nella scheda **Criteri**. L'icona che indica lo stato del criterio (attivo/inattivo) viene visualizzata prima del nome del criterio. È possibile creare più criteri per applicazioni differenti in un solo gruppo. Un solo criterio per ogni applicazione può essere attivo. Quando si crea un nuovo criterio attivo, il criterio attivo precedente diventa inattivo.

È possibile modificare un criterio dopo averlo creato.

Per creare un criterio di gruppo per la gestione dei dispositivi mobili:

1. Nella struttura di Console selezionare il gruppo di amministrazione per cui creare un criterio.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Fare clic sul collegamento **Crea criterio** per avviare la Creazione guidata nuovo criterio.

   Verrà avviata la Creazione guidata nuovo criterio.

Passaggio 1. Scegliere un'applicazione per la creazione di un criterio di gruppo

Durante questo passaggio, selezionare l'applicazione per cui si desidera creare un criterio di gruppo nell'elenco delle applicazioni:

- **Kaspersky Endpoint Security for Android** – per i dispositivi che utilizzano l'app mobile Kaspersky Endpoint Security for Android.

  È consigliabile creare un criterio separato per i dispositivi Huawei e Honor che non dispongono dei servizi Google Play. In questo modo è possibile inviare collegamenti a Huawei AppGallery agli utenti di tali dispositivi.

- **Kaspersky Device Management for iOS** – per i dispositivi EAS e MDM iOS.

  Un criterio per i dispositivi mobili può essere creato se il plug-in di amministrazione di Kaspersky Endpoint Security for Android e il plug-in di amministrazione di Kaspersky Device Management for iOS sono installati nel desktop dell'amministratore. Se i plug-in non sono installati, il nome dell'applicazione corrispondente non viene visualizzato nell'elenco delle applicazioni.

Proseguire con il passaggio successivo della Creazione guidata nuovo criterio.

Passaggio 2. Immettere il nome di un criterio di gruppo

Durante questo passaggio, digitare il nome del nuovo criterio nel campo **Nome**. Se si specifica il nome di un criterio esistente, al nome del nuovo criterio verrà automaticamente aggiunto (1) alla fine.

Proseguire con il passaggio successivo della Creazione guidata nuovo criterio.

Passaggio 3. Creare un criterio di gruppo per l'applicazione

Durante questo passaggio, la procedura guidata richiede di selezionare lo stato del criterio.

- **Criterio attivo**. La procedura guidata salva il criterio creato nell'Administration Server. Alla successiva sincronizzazione del dispositivo mobile con l'Administration Server, il criterio verrà utilizzato nel dispositivo come criterio attivo.

- **Criterio inattivo.** La procedura guidata salva il criterio creato nell'Administration Server come criterio di backup. Questo criterio può essere attivato in futuro dopo un evento specifico. Se necessario, un criterio inattivo può essere impostato come attivo.

  È possibile creare diversi criteri per un'applicazione nel gruppo, ma solo uno può essere attivo. Quando si crea un nuovo criterio attivo, il criterio attivo precedente diventa automaticamente inattivo.

Uscire dalla procedura guidata.

Configurazione delle impostazioni di sincronizzazione

Per gestire i dispositivi mobili e ricevere rapporti o statistiche dai dispositivi mobili degli utenti, è necessario configurare le impostazioni di sincronizzazione. La sincronizzazione dei dispositivi mobili con Kaspersky Security Center può essere eseguita nei seguenti modi:

- **In base alla pianificazione**. La sincronizzazione in base alla pianificazione viene eseguita tramite il protocollo HTTP. È possibile configurare la pianificazione della sincronizzazione nelle impostazioni dei criteri di gruppo. Le modifiche apportate alle impostazioni dei criteri di gruppo, a comandi e attività verranno eseguite durante la sincronizzazione del dispositivo con Kaspersky Security Center in base alla pianificazione, e quindi con un ritardo. Per impostazione predefinita, i dispositivi mobili vengono sincronizzati automaticamente con Kaspersky Security Center ogni 6 ore.

  In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

- **Forzata**. La sincronizzazione forzata viene eseguita utilizzando le notifiche push del servizio FCM (Firebase Cloud Messaging). La sincronizzazione forzata è orientata principalmente all'invio tempestivo dei comandi a un dispositivo mobile. Se si desidera utilizzare la sincronizzazione forzata, assicurarsi che le impostazioni GSM siano configurate in Kaspersky Security Center. Per ulteriori informazioni, fare riferimento alla Guida di Kaspersky Security Center.

Per configurare le impostazioni di sincronizzazione del dispositivo mobile con Kaspersky Security Center:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Sincronizzazione**.

5. Selezionare la frequenza di sincronizzazione nell'elenco a discesa **Sincronizza**.

6. Per disabilitare la sincronizzazione di un dispositivo con Kaspersky Security Center durante il roaming, selezionare la casella **Non sincronizzare in roaming**.

   L'utente del dispositivo può eseguire manualmente la sincronizzazione nelle impostazioni dell'app (→ **Impostazioni** → **Sincronizzazione** → **Sincronizza**).

7. Per nascondere all'utente le impostazioni di sincronizzazione (indirizzo del server, porta e gruppo di amministrazione) nelle impostazioni dell'app, deselezionare la casella **Mostra impostazioni di sincronizzazione nel dispositivo**. È impossibile modificare le impostazioni nascoste.

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. È possibile sincronizzare manualmente il dispositivo mobile utilizzando un comando specifico. Per sapere di più su come utilizzare i comandi per dispositivi mobili, fare riferimento alla *Guida di Kaspersky Security Center*.

Gestione delle revisioni dei criteri di gruppo

Kaspersky Security Center consente di tenere traccia delle modifiche apportate ai criteri di gruppo. Ogni volta che si salvano le modifiche apportate a un criterio di gruppo, viene creata una *revisione*. Ogni revisione è contrassegnata da un numero.

È possibile gestire le revisioni solo per i criteri di Kaspersky Endpoint Security for Android. Non è possibile gestire le revisioni per i criteri di Kaspersky Device Management for iOS.

È possibile eseguire le seguenti operazioni sulle revisioni dei criteri di gruppo:

- Confrontare una revisione selezionata con quella corrente.
- Confrontare le revisioni selezionate.
- Confrontare un criterio con una revisione selezionata di un altro criterio.
- Visualizzare una revisione selezionata.
- Eseguire il rollback delle modifiche di un criterio a una revisione selezionata.
- Salvare le revisioni in un file .txt.

Per maggiori dettagli sulla gestione delle revisioni dei criteri di gruppo e di altri oggetti (ad esempio degli account utente), fare riferimento alla *Guida di Kaspersky Security Center*.

Per visualizzare la cronologia delle revisioni dei criteri di gruppo:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Cronologia revisioni**.

   Verrà visualizzato un elenco di revisioni dei criteri. Contiene le seguenti informazioni:

   - Numero di revisione del criterio
   - Data e ora di modifica del criterio
   - Nome dell'utente che ha modificato il criterio

- Azione eseguita sul criterio
- Descrizione della revisione apportata alle impostazioni del criterio

Rimozione di un criterio di gruppo

Per rimuovere un criterio di gruppo:

1. Nella struttura di Administration Console selezionare il gruppo di amministrazione per cui rimuovere un criterio.
2. Nell'area di lavoro del gruppo di amministrazione, nella scheda **Criteri**, selezionare il criterio da rimuovere.
3. Dal menu di scelta rapida del criterio selezionare **Elimina**.

Come risultato, il criterio di gruppo viene eliminato. Prima che venga applicato il nuovo criterio di gruppo, i dispositivi mobili che appartengono al gruppo di amministrazione continuano a funzionare con le impostazioni specificate nel criterio eliminato.

Limitazione delle autorizzazioni di configurazione dei criteri di gruppo

Gli amministratori di Kaspersky Security Center possono configurare le autorizzazioni di accesso degli utenti di Administration Console per le diverse funzioni della soluzione integrata Kaspersky Security for Mobile a seconda delle mansioni degli utenti.

Nell'interfaccia di Administration Console è possibile configurare i diritti di accesso nella finestra delle proprietà di Administration Server, nelle schede **Sicurezza** e **Ruoli utente**. La scheda **Ruoli utente** consente di aggiungere ruoli utente standard con un set di diritti predefinito. La sezione **Sicurezza** consente di configurare i diritti per un utente o un gruppo di utenti o di assegnare ruoli a un utente o a un gruppo di utenti. I diritti utente per ogni applicazione sono configurati in base agli *ambiti funzionali*.

È anche possibile configurare specifiche autorizzazioni utente per le varie aree funzionali. Le informazioni sulla corrispondenza tra le aree funzionali e le schede del criterio sono contenute nell'Appendice.

Per ogni area funzionale, l'amministratore può assegnare le seguenti autorizzazioni:

- **Consenti la modifica**. L'utente di Administration Console può modificare le impostazioni dei criteri nella finestra delle proprietà.
- **Blocca la modifica**. L'utente di Administration Console non può modificare le impostazioni dei criteri nella finestra delle proprietà. Le schede dei criteri che appartengono all'ambito funzionale per cui il diritto è stato assegnato non vengono visualizzate nell'interfaccia.

Per ulteriori dettagli sulla gestione di diritti e ruoli degli utenti in Administration Console di Kaspersky Security Center, vedere la *Guida di Kaspersky Security Center*.

Protezione

Questa sezione contiene informazioni su come gestire in remoto la protezione dei dispositivi mobili in Administration Console di Kaspersky Security Center.

Configurazione della protezione anti-virus nei dispositivi Android

Per il rilevamento tempestivo di minacce, virus e altre applicazioni dannose, è necessario configurare le impostazioni per la protezione in tempo reale e l'esecuzione automatica delle scansioni virus.

Kaspersky Endpoint Security for Android rileva i seguenti tipi di oggetti:

- Virus, worm, Trojan e strumenti dannosi
- Adware
- App che possono essere sfruttate da utenti malintenzionati per danneggiare il dispositivo o i dati personali

Anti-virus presenta diverse limitazioni:

- Quando Anti-Virus è in esecuzione, una minaccia rilevata nella memoria esterna del dispositivo (ad esempio una scheda SD) non può essere neutralizzata automaticamente nel profilo lavoro (Applicazioni con icona a forma di valigia, Configurazione del profilo lavoro Android). Kaspersky Endpoint Security for Android non ha accesso alla memoria esterna nel profilo lavoro. Le informazioni sugli oggetti rilevati vengono visualizzate nella sezione **Stato** dell'app. Per neutralizzare gli oggetti rilevati nella memoria esterna, i file dell'oggetto devono essere eliminati manualmente e la scansione del dispositivo deve essere riavviata.
- A causa di limitazioni tecniche, Kaspersky Endpoint Security for Android non può esaminare file con dimensioni pari o superiori a 2 GB. Durante una scansione, l'app ignora tali file senza inviare una notifica in merito.

Per configurare le impostazioni di protezione in tempo reale dei dispositivi mobili:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Protezione**.
5. Nella sezione **Protezione** configurare le impostazioni di protezione del file system del dispositivo mobile:
   - Per abilitare la protezione in tempo reale del dispositivo mobile dalle minacce, selezionare la casella **Abilita protezione**.

     Kaspersky Endpoint Security for Android esamina solo le nuove app e i nuovi file della cartella Download.
   - Per abilitare la protezione estesa del dispositivo mobile dalle minacce, selezionare la casella **Modalità di protezione estesa**.

     Kaspersky Endpoint Security for Android eseguirà la scansione di tutti i file aperti, modificati, spostati, copiati, installati o salvati dall'utente nel dispositivo e di tutte le nuove app mobili installate.

     Nei dispositivi con sistema operativo Android 8.0 o versione successiva, Kaspersky Endpoint Security for Android esamina i file modificati, spostati, installati e salvati dall'utente, nonché le copie dei file. Kaspersky Endpoint Security for Android non esamina i file quando vengono aperti, né i file di origine quando vengono copiati.

- Per abilitare la scansione aggiuntiva delle nuove app prima del primo avvio nel dispositivo dell'utente tramite il servizio cloud Kaspersky Security Network, selezionare la casella **Protezione cloud (KSN)**.

- Per bloccare adware e app che possono essere sfruttati da utenti malintenzionati per danneggiare il dispositivo o i dati dell'utente, selezionare la casella di controllo **Rileva adware, autodialer e app che possono essere utilizzati da utenti malintenzionati per danneggiare il dispositivo e i dati dell'utente**.

6. Nell'elenco **Azione se viene rilevata una minaccia** selezionare una delle seguenti opzioni:

   - **Elimina**

     Gli oggetti rilevati verranno eliminati automaticamente. All'utente non è richiesto di eseguire azioni aggiuntive. Prima di eliminare un oggetto, Kaspersky Endpoint Security for Android visualizzerà una notifica provvisoria sul rilevamento dell'oggetto.

   - **Ignora**

     Se gli oggetti rilevati sono stati ignorati, Kaspersky Endpoint Security for Android avvisa l'utente dei problemi di protezione del dispositivo. Le informazioni sugli oggetti ignorati vengono visualizzate nella sezione **Stato** dell'app. Per ogni minaccia ignorata, l'app propone azioni che l'utente può eseguire per eliminare la minaccia. L'elenco degli oggetti ignorati può ad esempio cambiare se un file dannoso è stato eliminato o spostato. Per ricevere un elenco aggiornato delle minacce, eseguire una scansione completa del dispositivo. Per garantire la protezione ottimale dei dati, eliminare tutti gli oggetti rilevati.

   - **Quarantena**

7. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Per configurare l'esecuzione automatica delle scansioni virus nel dispositivo mobile:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Scansione**.

5. Per bloccare adware e app che possono essere sfruttati da utenti malintenzionati per danneggiare il dispositivo o i dati dell'utente, selezionare la casella di controllo **Rileva adware, autodialer e app che possono essere utilizzati da utenti malintenzionati per danneggiare il dispositivo e i dati dell'utente**.

6. Nell'elenco **Azione se viene rilevata una minaccia** selezionare una delle seguenti opzioni:

   - **Elimina**

     Gli oggetti rilevati verranno eliminati automaticamente. All'utente non è richiesto di eseguire azioni aggiuntive. Prima di eliminare un oggetto, Kaspersky Endpoint Security for Android visualizzerà una notifica provvisoria sul rilevamento dell'oggetto.

   - **Ignora**

Se gli oggetti rilevati sono stati ignorati, Kaspersky Endpoint Security for Android avvisa l'utente dei problemi di protezione del dispositivo. Le informazioni sugli oggetti ignorati vengono visualizzate nella sezione **Stato** dell'app. Per ogni minaccia ignorata, l'app propone azioni che l'utente può eseguire per eliminare la minaccia. L'elenco degli oggetti ignorati può ad esempio cambiare se un file dannoso è stato eliminato o spostato. Per ricevere un elenco aggiornato delle minacce, eseguire una scansione completa del dispositivo. Per garantire la protezione ottimale dei dati, eliminare tutti gli oggetti rilevati.

- **Quarantena**
- **Chiedi all'utente**

  L'app Kaspersky Endpoint Security for Android visualizza una notifica che richiede all'utente di scegliere l'azione da eseguire sull'oggetto rilevato: **Ignora** o **Elimina**.

  Quando l'app rileva più oggetti, l'opzione **Chiedi all'utente** consente all'utente del dispositivo di applicare un'azione selezionata a ogni file utilizzando la casella **Applica a tutti**.

Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità al fine di garantire la visualizzazione delle notifiche nei dispositivi mobili che eseguono Android 10.0 o versioni successive. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo. In questo caso Kaspersky Endpoint Security for Android visualizza una finestra di sistema Android che richiede all'utente di scegliere l'azione da eseguire sull'oggetto rilevato: Ignora o Elimina. Per applicare un'azione a più oggetti, è necessario aprire Kaspersky Endpoint Security.

7. La sezione **Scansione pianificata** consente di configurare le impostazioni per l'avvio automatico della scansione completa del file system del dispositivo. A tale scopo, fare clic sul pulsante **Pianificazione** e specificare la frequenza e l'ora di avvio della scansione completa nella finestra **Pianificazione**.

   In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. Kaspersky Endpoint Security for Android esamina tutti i file, compresi i contenuti degli archivi.

Per mantenere aggiornata la protezione del dispositivo mobile, configurare le impostazioni di aggiornamento dei database anti-virus.

Per impostazione predefinita, gli aggiornamenti dei database anti-virus sono disabilitati quando il dispositivo è in roaming. Gli aggiornamenti pianificati dei database anti-virus non vengono eseguiti.

Per configurare le impostazioni di aggiornamento dei database anti-virus:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Aggiornamento database**.

5. Se si desidera che Kaspersky Endpoint Security for Android scarichi gli aggiornamenti dei database in base alla pianificazione quando il dispositivo è nell'area di roaming, selezionare la casella **Consenti aggiornamento dei database in roaming** nella sezione **Aggiornamento dei database in roaming**.

   Anche se la casella è deselezionata, l'utente può avviare manualmente l'aggiornamento dei database anti-virus quando il dispositivo è in roaming.

6. Nella sezione **Sorgente degli aggiornamenti dei database** specificare la sorgente degli aggiornamenti da cui Kaspersky Endpoint Security for Android riceve e installa gli aggiornamenti dei database anti-virus:

   - **Server di Kaspersky**

     Utilizzo di un server di aggiornamento di Kaspersky come sorgente degli aggiornamenti per scaricare i database di Kaspersky Endpoint Security for Android nei dispositivi mobili degli utenti. Per aggiornare i database dai server di Kaspersky, Kaspersky Endpoint Security for Android trasmette dati a Kaspersky (ad esempio, l'ID di esecuzione dell'attività di aggiornamento). L'elenco dei dati trasmessi durante gli aggiornamenti dei database è riportato nel Contratto di licenza con l'utente finale.

   - **Administration Server**

     Utilizzo dell'archivio di Kaspersky Security Center Administration Server come sorgente degli aggiornamenti per scaricare i database di Kaspersky Endpoint Security for Android nei dispositivi mobili degli utenti.

   - **Altra sorgente**

     Utilizzo di un server di terze parti come sorgente degli aggiornamenti per scaricare i database di Kaspersky Endpoint Security for Android nei dispositivi mobili degli utenti. Per avviare un aggiornamento, è necessario inserire l'indirizzo di un server HTTP nel campo sottostante (ad esempio, http://dominio.com/).

7. Nella sezione **Aggiornamento dei database pianificato** configurare le impostazioni per gli aggiornamenti automatici dei database anti-virus nel dispositivo dell'utente. A tale scopo, fare clic sul pulsante **Pianificazione** e specificare la frequenza e l'ora di avvio degli aggiornamenti nella finestra **Pianificazione**.

   In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Protezione dei dispositivi Android su Internet

Per proteggere i dati personali dell'utente di un dispositivo mobile su Internet, abilitare Protezione Web. Protezione Web blocca i siti Web dannosi che distribuiscono codice dannoso e i siti Web di phishing progettati per rubare le informazioni riservate dell'utente e ottenere l'accesso ai conti personali. Protezione Web analizza i siti Web prima dell'apertura utilizzando il servizio cloud Kaspersky Security Network. Protezione Web consente inoltre di configurare l'accesso di un utente ai siti Web in base a elenchi predefiniti di siti Web consentiti e bloccati.

Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo.

Protezione Web nei dispositivi Android funziona solo nel browser Google Chrome (inclusa la funzionalità Schede personalizzate), in Huawei Browser e Samsung Internet Browser. Protezione Web per Samsung Internet Browser non blocca i siti su un dispositivo mobile se viene utilizzato un profilo lavoro e Protezione Web è abilitato solo per il profilo lavoro.

Per abilitare Protezione Web in Google Chrome, Huawei Browser, or Samsung Internet Browser:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare **Protezione Web**.
5. Per utilizzare Protezione Web, l'utente o l'utente del dispositivo deve leggere e accettare l'Informativa relativa all'elaborazione dei dati a scopo di utilizzo di Protezione Web (Informativa di Protezione Web):
   a. Fare clic sul collegamento **Informativa di Protezione Web**.

      Viene visualizzata la finestra **Informativa relativa all'elaborazione dei dati a scopo di utilizzo di Protezione Web**. Per accettare l'Informativa di Protezione Web, è necessario leggere e accettare l'Informativa sulla privacy.

   b. Fare clic sul collegamento dell'Informativa sulla privacy. Leggere e accettare l'Informativa sulla privacy.

      Se non si accetta l'Informativa sulla privacy, l'utente del dispositivo mobile può accettare l'Informativa sulla privacy nella Configurazione iniziale guidata o nell'app (→ **Informazioni sull'app** → **Termini e condizioni** → **Informativa sulla privacy**).

   c. Selezionare la modalità di accettazione dell'Informativa di Protezione Web:

      - **Ho letto e accetto l'Informativa di Protezione Web**
      - **Richiedi l'accettazione dell'Informativa di Protezione Web da parte dell'utente del dispositivo**
      - **Non accetto l'Informativa di Protezione Web**
6. Se si seleziona **Non accetto l'Informativa di Protezione Web**, Protezione Web non blocca i siti in un dispositivo mobile. L'utente del dispositivo mobile non può abilitare Protezione Web in Kaspersky Endpoint Security.
7. Selezionare la casella **Abilita Protezione Web**.
8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Protezione dei dati di un dispositivo rubato o smarrito

In questa sezione viene descritto come configurare le impostazioni della protezione dall'accesso non autorizzato nel dispositivo in caso di furto o smarrimento.

Invio dei comandi a un dispositivo mobile

Per proteggere i dati in un dispositivo mobile in caso di furto o smarrimento, è possibile inviare comandi speciali (vedere la tabella di seguito).

Comandi per la protezione dei dati in un dispositivo smarrito o rubato

Metodo di connessione a Kaspersky Security Center	Comando	Risultato di esecuzione del comando
Kaspersky Endpoint Security for Android	Blocca	Il dispositivo mobile è bloccato.
	Sblocca	Dopo aver sbloccato un dispositivo mobile che esegue Android 5.0 - 6.X, la password di sblocco dello schermo (codice PIN) viene reimpostata su "1234". Dopo aver sbloccato un dispositivo che esegue Android 7.0 o versioni successive, la password di sblocco dello schermo non viene modificata.
	Localizzazione dispositivo	Il dispositivo viene localizzato e visualizzato su Google Maps. Il fornitore di servizi mobili applica una tariffa per l'invio del messaggio SMS e per l'accesso a Internet. Nei dispositivi che eseguono Android 12 o versioni successive, se l'utente ha concesso l'autorizzazione per l'utilizzo della posizione approssimativa, l'app Kaspersky Endpoint Security for Android cerca prima di ottenere la posizione esatta del dispositivo. Se l'operazione non va a buon fine, viene restituita la posizione approssimativa del dispositivo solo se è stata ricevuta non più di 30 minuti prima. In caso contrario, il comando di **Localizza dispositivo** non va a buon fine.
	Foto utente	Il dispositivo mobile è bloccato. La foto utente viene scattata dalla fotocamera anteriore del dispositivo quando qualcuno tenta di sbloccare il dispositivo. Il fornitore di servizi mobili applica una tariffa per l'invio del messaggio SMS e per l'accesso a Internet. Tentando di sbloccare il dispositivo, l'utente acconsente automaticamente alla foto utente. Se l'autorizzazione per l'utilizzo della fotocamera è stata revocata, il dispositivo mobile visualizza una notifica e richiede di fornire l'autorizzazione. In un dispositivo mobile con Android 12 o versione successiva, se l'autorizzazione per l'utilizzo della fotocamera è stata revocata tramite le impostazioni rapide, la notifica non viene visualizzata ma la foto scattata risulta nera.
	Allarme	Il dispositivo mobile emette un tono di allarme. L'allarme suona per 5 minuti (o per 1 minuto se la batteria del dispositivo è scarica).
	Cancella dati aziendali	Cancellare i dati inseriti in un contenitore, account e-mail aziendale, impostazioni per la connessione alla rete Wi-Fi aziendale e alla VPN, nome

		del punto di accesso (APN), profilo lavoro Android, contenitore KNOX e chiave di gestione delle licenze KNOX.
	Ripristina le impostazioni predefinite	Tutti i dati vengono eliminati dal dispositivo mobile e viene eseguito il rollback delle impostazioni ai valori predefiniti. Dopo l'esecuzione del comando, il dispositivo non sarà in grado di ricevere o eseguire i comandi successivi.
Profilo MDM iOS	Blocca	Il dispositivo mobile è bloccato.
	Sblocca	Il blocco del dispositivo mobile con un codice PIN è disabilitato. Il codice PIN precedentemente specificato è stato reimpostato.
	Cancella dati aziendali	Tutti i profili di configurazione installati, i profili di provisioning, il profilo MDM iOS e le applicazioni per cui è stata selezionata la casella **Rimuovi insieme al profilo MDM iOS** vengono rimossi dal dispositivo.
	Ripristina le impostazioni predefinite	Tutti i dati vengono eliminati dal dispositivo mobile e viene eseguito il rollback delle impostazioni ai valori predefiniti. Dopo l'esecuzione del comando, il dispositivo non sarà in grado di ricevere o eseguire i comandi successivi.
Cassetta postale Exchange	Ripristina le impostazioni predefinite	Tutti i dati vengono eliminati dal dispositivo mobile e viene eseguito il rollback delle impostazioni ai valori predefiniti. Dopo l'esecuzione del comando, il dispositivo non sarà in grado di ricevere o eseguire i comandi successivi.

Per l'esecuzione dei comandi di Kaspersky Endpoint Security for Android sono richiesti diritti e autorizzazioni speciali. Durante l'esecuzione della procedura guidata di configurazione iniziale, Kaspersky Endpoint Security for Android richiede all'utente di concedere all'applicazione tutti i diritti e le autorizzazioni richiesti. L'utente può ignorare questi passaggi o disabilitare tali autorizzazioni nelle impostazioni del dispositivo in un momento successivo. In tal caso, non sarà possibile eseguire i comandi.

Nei dispositivi che eseguono Android 10.0 o versioni successive, l'utente deve concedere l'autorizzazione "Sempre" per accedere alla posizione. Nei dispositivi che eseguono Android 11.0 o versioni successive, l'utente deve inoltre concedere l'autorizzazione "Durante l'utilizzo dell'app" per accedere alla fotocamera. In caso contrario, i comandi di Antifurto non funzioneranno. L'utente verrà informato di questa limitazione e gli verrà nuovamente richiesto di concedere le autorizzazioni del livello richiesto. Se l'utente seleziona l'opzione "Solo questa volta" per l'autorizzazione relativa alla fotocamera, si ritiene che l'accesso sia concesso dall'app. È consigliabile contattare direttamente l'utente se viene richiesta nuovamente l'autorizzazione relativa alla fotocamera.

Per sapere di più su come inviare comandi dall'elenco di dispositivi mobili in Administration Console, fare riferimento alla *Guida di Kaspersky Security Center*.

Sblocco di un dispositivo mobile

È possibile sbloccare un dispositivo mobile utilizzando i seguenti metodi:

- Inviare il comando di sblocco al dispositivo mobile.
- Immettere la password di sblocco monouso nel dispositivo mobile (solo per dispositivi Android).

In determinati dispositivi (ad esempio Huawei, Meizu e Xiaomi), è necessario aggiungere manualmente Kaspersky Endpoint Security for Android all'elenco delle app eseguite all'avvio del sistema operativo. Se l'app non è stata aggiunta all'elenco, è possibile sbloccare il dispositivo solo utilizzando una password di sblocco monouso. Non è possibile utilizzare i comandi per sbloccare il dispositivo.

Per sapere di più su come inviare comandi dall'elenco di dispositivi mobili in Administration Console, fare riferimento alla *Guida di Kaspersky Security Center*.

Per *password di sblocco monouso* si intende una password segreta dell'applicazione per lo sblocco del dispositivo mobile. La password monouso viene generata dall'applicazione ed è univoca per ogni dispositivo mobile. È possibile modificare la lunghezza della password monouso (4, 8 o 16 cifre) nelle impostazioni del criterio di gruppo nella sezione **Antifurto**.

Per sbloccare il dispositivo mobile utilizzando una password monouso:

1. Nella struttura della console selezionare **Mobile Device Management** → **Dispositivi mobili**.
2. Selezionare un dispositivo mobile per cui si desidera ottenere una password di sblocco monouso.
3. Aprire la finestra delle proprietà del dispositivo mobile facendo doppio clic.
4. Selezionare **App** → **Kaspersky Endpoint Security for Android**.
5. Aprire la finestra delle proprietà di Kaspersky Endpoint Security facendo doppio clic.
6. Selezionare la sezione **Antifurto**.
7. Una password univoca per il dispositivo selezionato verrà visualizzata nel campo **Password monouso** della sezione **Password monouso di sblocco del dispositivo**.
8. Utilizzare qualsiasi metodo disponibile (ad esempio e-mail) per comunicare la password monouso all'utente del dispositivo bloccato.
9. L'utente immette la password monouso nella schermata del dispositivo bloccato da Kaspersky Endpoint Security for Android.

Il dispositivo mobile verrà sbloccato. Dopo aver sbloccato un dispositivo mobile che esegue Android 5.0 - 6.X, la password di sblocco dello schermo (codice PIN) viene reimpostata su "1234". Dopo aver sbloccato un dispositivo che esegue Android 7.0 o versioni successive, la password di sblocco dello schermo non viene modificata.

Criptaggio dei dati

Per proteggere i dati dall'accesso non autorizzato, è necessario abilitare il criptaggio di tutti i dati nel dispositivo (ad esempio, credenziali di account, dispositivi esterni e app, oltre che messaggi e-mail, messaggi SMS, contatti, foto e altri file). Per accedere ai dati criptati, è necessario specificare una speciale chiave: la password di sblocco del dispositivo. Se i dati sono criptati, è possibile accedervi solo quando il dispositivo viene sbloccato.

Il criptaggio dei dati è abilitato per impostazione predefinita nei dispositivi iOS bloccati tramite password (**Impostazioni** → **Touch ID / Face ID e Password** → **Abilita password**).

Per criptare tutti i dati in un dispositivo Android:

1. Abilitare il blocco dello schermo nel dispositivo Android (**Impostazioni** → **Sicurezza** → **Blocco dello schermo**).

2. Impostare una password di sblocco del dispositivo conforme ai requisiti di sicurezza aziendali.

   Non è consigliabile utilizzare un blocco tramite sequenza per sbloccare il dispositivo. In determinati dispositivi Android che eseguono Android 6.0 o versione successiva, dopo il criptaggio dei dati e il riavvio del dispositivo Android è necessario immettere una password numerica per sbloccare il dispositivo anziché un blocco tramite sequenza. Questo problema è correlato all'esecuzione del servizio per le funzionalità di accessibilità. In questo caso, per sbloccare lo schermo del dispositivo convertire il blocco tramite sequenza in una password numerica. Per maggiori informazioni sulla conversione di un blocco tramite sequenza in una password numerica, fare riferimento al sito Web dell'Assistenza tecnica del produttore del dispositivo mobile.

3. Abilitare il criptaggio di tutti i dati nel dispositivo (**Impostazioni** → **Sicurezza** → **Cripta dati**).

Configurazione della complessità della password di sblocco del dispositivo

Per proteggere l'accesso al dispositivo mobile di un utente, è necessario impostare una password di sblocco del dispositivo.

Questa sezione contiene informazioni su come configurare la protezione tramite password nei dispositivi iOS e Android.

Configurazione di una password di sblocco complessa per un dispositivo Android

Per mantenere protetto un dispositivo Android, è necessario configurare l'utilizzo di una password richiesta all'utente quando il dispositivo esce dalla modalità di sospensione.

È possibile imporre restrizioni sull'attività dell'utente nel dispositivo se la password di sblocco è vulnerabile (ad esempio il blocco del dispositivo). È possibile imporre restrizioni utilizzando il componente Controllo conformità. A tale scopo, nelle impostazioni delle regole di scansione è necessario selezionare il criterio **La password di sblocco non è conforme ai requisiti di sicurezza**.

In alcuni dispositivi Samsung con Android 7.0 o versioni successive, quando l'utente tenta di configurare metodi non supportati per lo sblocco del dispositivo (ad esempio, una password grafica), il dispositivo può essere bloccato se vengono soddisfatte le seguenti condizioni: la protezione dalla rimozione di Kaspersky Endpoint Security for Android è abilitata e sono impostati requisiti per la complessità della password di sblocco dello schermo. Per sbloccare il dispositivo, è necessario inviare un comando speciale al dispositivo.

Per configurare l'utilizzo di una password di sblocco:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Gestione dispositivo**.

5. Se si desidera che l'app controlli se è impostata o meno una password di sblocco, selezionare la casella **Richiedi di impostare una password di sblocco dello schermo** nella sezione **Blocco dello schermo**.

   Se l'applicazione rileva che nel dispositivo non è stata impostata alcuna password di sistema, richiede all'utente di impostarla. La password viene impostata secondo i parametri definiti dall'amministratore.

6. Specificare il numero minimo di caratteri.

   Numero minimo di caratteri per la password dell'utente. Valori possibili: da 4 a 16 caratteri.

   La password dell'utente è composta da 4 caratteri per impostazione predefinita.

   Nei dispositivi che eseguono Android 10.0 o versioni successive Kaspersky Endpoint Security risolve i requisiti di complessità della password in uno dei valori di sistema: medio o alto.

   I valori per i dispositivi che eseguono Android 10.0 o versioni successive sono determinati dalle seguenti regole:

   - Se la lunghezza della password richiesta è compresa tra 1 e 4 simboli, l'app richiede all'utente di impostare una password di complessità media. Deve essere una password numerica (PIN) senza sequenze ripetute o ordinate (ad es. 1234) oppure alfabetica/alfanumerica. Il PIN o la password deve contenere almeno 4 caratteri.

   - Se la lunghezza della password richiesta è superiore a 5 simboli, l'app richiede all'utente di impostare una password di complessità alta. Deve essere una password numerica (PIN) senza sequenze ripetute o ordinate oppure alfabetica/alfanumerica (password). Il PIN deve contenere almeno 8 cifre; la password deve contenere almeno 6 caratteri.

7. Se si desidera consentire all'utente di utilizzare le impronte digitali per lo sblocco dello schermo, selezionare la casella **Consenti l'utilizzo delle impronte digitali**. Se la password di sblocco non rispetta i requisiti di sicurezza aziendali, non è possibile utilizzare un lettore di impronte digitali per sbloccare lo schermo.

   Nei dispositivi che eseguono Android 10.0 o versioni successive l'uso dell'impronta digitale per sbloccare lo schermo può essere gestito solo per il profilo lavoro.

   Kaspersky Endpoint Security for Android non limita l'utilizzo di un lettore di impronte digitali per l'accesso alle app o la conferma degli acquisti

   In determinati dispositivi Samsung, non è possibile impedire l'utilizzo delle impronte digitali per lo sblocco dello schermo. In determinati dispositivi Samsung, se la password di sblocco non è conforme ai requisiti di sicurezza aziendali, Kaspersky Endpoint Security for Android non impedisce l'utilizzo delle impronte digitali per lo sblocco dello schermo.

   Dopo aver aggiunto un'impronta digitale nelle impostazioni del dispositivo, l'utente può sbloccare lo schermo utilizzando i seguenti metodi:

   - Posizionare il dito sul lettore di impronte digitali (metodo principale).

   - Immettere la password di sblocco (metodo secondario).

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione di una password di sblocco complessa per i dispositivi MDM iOS

Per proteggere i dati dei dispositivi MDM iOS, configurare le impostazioni per la complessità della password di sblocco.

Per impostazione predefinita, l'utente può utilizzare una password semplice. Una *password semplice* è una password che contiene caratteri successivi o ripetuti, come "abcd" o "2222". All'utente non viene richiesto di immettere una password alfanumerica che include simboli speciali. Per impostazione predefinita, il periodo di validità della password e il numero di tentativi di immissione della password non sono limitati.

Per configurare le impostazioni della complessità di una password di sblocco dei dispositivi MDM iOS:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Password**.
5. Nella sezione **Impostazioni password** selezionare la casella **Applica impostazioni nel dispositivo**.
6. Configurare le impostazioni per la complessità della password di sblocco:
   - Per consentire all'utente di utilizzare una password semplice, selezionare la casella **Consenti password semplice**.
   - Per richiedere l'utilizzo sia di lettere che di numeri nella password, selezionare la casella **Richiedi valore alfanumerico**.
   - Nell'elenco **Lunghezza minima password** selezionare la lunghezza minima password in caratteri.
   - Nell'elenco **Numero minimo di caratteri speciali** selezionare il numero minimo di caratteri speciali nella password (ad esempio, "$", "&", "!").
   - Nel campo **Durata massima della password** specificare il periodo di tempo in giorni per cui la password resterà valida. Al termine di questo periodo, Kaspersky Device Management for iOS richiede all'utente di modificare la password.
   - Nell'elenco **Abilita blocco automatico** selezionare il periodo di tempo dopo il quale deve essere abilitato il blocco automatico del dispositivo MDM iOS.
   - Nel campo **Cronologia password** specificare il numero di password già utilizzate (inclusa la password corrente) che Kaspersky Device Management for iOS confronta con la nuova password quando l'utente modifica la password precedente. Se le password corrispondono, la nuova password viene rifiutata.
   - Nell'elenco **Tempo di sblocco massimo senza password** selezionare il periodo di tempo per cui l'utente può sbloccare il dispositivo MDM iOS senza immettere la password.
   - In **Numero massimo di tentativi di accesso** selezionare il numero di tentativi di accesso che l'utente può effettuare per immettere la password di sblocco del dispositivo MDM iOS.
7. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, Kaspersky Device Management for iOS verifica la complessità della password nel dispositivo mobile dell'utente. Se la complessità della password di sblocco del dispositivo non è conforme al criterio, all'utente viene richiesto di modificare la password.

Configurazione di una password di sblocco complessa per i dispositivi EAS

Impostare una password sblocco di complessa per proteggere i dati nei dispositivi EAS.

Per impostazione predefinita, quando il dispositivo mobile di un utente viene acceso, Kaspersky Device Management for iOS non richiede all'utente di inserire o impostare una password di sblocco.

Per configurare le impostazioni della complessità di una password di sblocco dei dispositivi EAS:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi EAS.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra Proprietà del criterio selezionare la sezione **Password**.
5. Nella sezione **Impostazioni password** selezionare la casella **Richiedi password**.
6. Configurare le impostazioni per la complessità della password di sblocco:
   - Per richiedere all'utente di utilizzare sia lettere che numeri nella password, selezionare la casella **Richiedi valore alfanumerico**. Nel campo **Numero minimo di caratteri** specificare il livello di complessità della password alfanumerica. Valori possibili: da 1 a 4. Il valore "1" corrisponde al livello di complessità più basso.
   - Per consentire all'utente di utilizzare la funzione di ripristino della password, selezionare la casella **Consenti il ripristino della password**.
   - Se si desidera criptare i file nella memoria del dispositivo, selezionare la casella **Richiedi il criptaggio del dispositivo**.
   - Se si desidera criptare i file nella scheda di memoria, selezionare la casella **Richiedi il criptaggio della scheda di memoria**.
   - Per consentire all'utente di utilizzare una password semplice che contiene solo numeri, selezionare la casella **Consenti password semplice**.
   - Per limitare il numero di tentativi di immissione della password per l'accesso al dispositivo, selezionare la casella **Numero massimo di tentativi di accesso**. Nel campo a destra della casella specificare il numero di tentativi di immissione della password che l'utente può eseguire per sbloccare il dispositivo. Se l'utente non immette la password corretta dopo il numero specificato di tentativi consecutivi, Kaspersky Device Management for iOS cancella tutti i dati sul dispositivo.
   - Per specificare la lunghezza minima della password dell'utente, selezionare la casella **Lunghezza minima password**. Specificare il numero minimo di caratteri della password nel campo a destra della casella. Valori possibili: da 4 a 16 caratteri.
   - Per richiedere all'utente di immettere la password dopo un determinato periodo di inattività del dispositivo, selezionare la casella **Tempo di inattività prima di un nuovo tentativo di immissione della password (min)**. Nel campo a destra della casella specificare il tempo di inattività in minuti. Al termine di questo periodo, l'applicazione richiede all'utente di immettere la password.

- Per il limitare il periodo di validità della password, selezionare la casella **Periodo di validità della password (giorni)**. Nel campo a destra della casella specificare il periodo di validità della password. Al termine di questo periodo, l'applicazione richiede all'utente di modificare la password.

- Nel campo **Cronologia password** specificare il numero delle password più recenti che non possono essere riutilizzate.

7. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. Una volta applicato il criterio, Kaspersky Device Management for iOS verifica se è impostata una password nel dispositivo mobile dell'utente. Se la password di sblocco non è impostata nel dispositivo, all'utente viene richiesto di impostarla. La password deve essere impostata tenendo conto delle impostazioni del criterio. Se la password di sblocco del dispositivo è impostata ma non è conforme al criterio, all'utente viene richiesto di modificare la password.

Configurazione di una rete privata virtuale (VPN)

Questa sezione contiene informazioni sulla configurazione delle impostazioni della rete privata virtuale (VPN) per la connessione sicura alle reti Wi-Fi.

Configurazione della VPN nei dispositivi Android (solo Samsung)

Per connettere in modo sicuro un dispositivo Android alle reti Wi-Fi e proteggere il trasferimento dei dati, è necessario configurare le impostazioni per la VPN (Virtual Private Network).

La configurazione della VPN è possibile solo per i dispositivi Samsung.

Durante l'utilizzo di una rete privata virtuale è necessario tenere presenti i seguenti requisiti:

- L'app che utilizza la connessione VPN deve essere consentita nelle impostazioni del firewall.

- Le impostazioni della rete privata virtuale configurate nel criterio non possono essere applicate alle applicazioni di sistema. La connessione VPN per le applicazioni di sistema deve essere configurata manualmente.

- Per alcune applicazioni che utilizzano la connessione VPN è necessario configurare impostazioni aggiuntive al primo avvio. Per configurare le impostazioni, la connessione VPN deve essere consentita nelle impostazioni dell'applicazione.

Per configurare la VPN nel dispositivo mobile di un utente:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Gestisci Samsung KNOX → Gestisci dispositivo Samsung**.

5. Nella sezione **VPN** fare clic sul pulsante **Configura**.

Verrà visualizzata la finestra **Rete VPN**.

6. Nell'elenco a discesa **Tipo di connessione** selezionare il tipo di connessione VPN.
7. Nel campo **Nome della rete** immettere il nome del tunnel VPN.
8. Nel campo **Indirizzo server** immettere il nome di rete o l'indirizzo IP del server VPN.
9. Nell'elenco **Domini di ricerca DNS** immettere il dominio di ricerca DNS da aggiungere automaticamente al nome DNS del server.

   È possibile specificare diversi domini di ricerca DNS, separati da spazi.
10. Nel campo **Server DNS** immettere il nome di dominio completo o l'indirizzo IP del server DNS.

    È possibile specificare diversi server DNS, separati da spazi.
11. Nel campo **Routing** immettere l'intervallo di indirizzi IP di rete con cui vengono scambiati dati tramite la connessione VPN.

    Se l'intervallo di indirizzi IP non è specificato nel campo **Routing**, tutto il traffico Internet attraverserà la connessione VPN.
12. Configurare inoltre le impostazioni seguenti per le reti di tipo **IPSec Xauth PSK** e **L2TP IPSec PSK**:

    a. Nel campo **Chiave condivisa IPSec** immettere la password per la chiave di sicurezza IPSec preimpostata.

    b. Nel campo **ID IPSec** immettere il nome dell'utente del dispositivo mobile.
13. Per una rete **L2TP IPSec PSK** è inoltre possibile specificare la password per la chiave L2TP nel campo **Chiave L2TP**.
14. Per una rete **PPTP** è possibile selezionare **Usa connessione SSL** in modo che l'app utilizzi il metodo di criptaggio dei dati MPPE (Microsoft Point-to-Point Encryption) per la protezione della trasmissione dei dati quando il dispositivo mobile si connette al server VPN.
15. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione della VPN nei dispositivi MDM iOS

Per connettere un dispositivo MDM iOS a una rete privata virtuale (VPN) e proteggere i dati durante la connessione alla VPN, configurare le impostazioni della connessione VPN.

Per configurare la connessione VPN nel dispositivo MDM iOS di un utente:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **VPN**.

5. Fare clic sul pulsante **Aggiungi** nella sezione **Reti VPN**.

   Verrà visualizzata la finestra **Rete VPN**.

6. Nel campo **Nome della rete** immettere il nome del tunnel VPN.

7. Nell'elenco a discesa **Tipo di connessione** selezionare il tipo di connessione VPN:

   - **L2TP** (Layer 2 Tunneling Protocol). La connessione supporta l'autenticazione dell'utente del dispositivo mobile MDM iOS tramite password MS-CHAP v2, autenticazione a due fattori e autenticazione automatica tramite una chiave pubblica.

   - **PPTP** (Point-to-Point Tunneling Protocol). La connessione supporta l'autenticazione dell'utente del dispositivo mobile MDM iOS tramite password MS-CHAP v2 e autenticazione a due fattori.

   - **IPSec (Cisco)**. La connessione supporta l'autenticazione dell'utente basata su password, l'autenticazione a due fattori e l'autenticazione automatica tramite una chiave pubblica e certificati.

   - **Cisco AnyConnect**. La connessione supporta il firewall Cisco Adaptive Security Appliance (ASA) versione 8.0(3).1 o successiva. Per configurare la connessione VPN, installare l'app Cisco AnyConnect dall'App Store nel dispositivo mobile MDM iOS.

   - **Juniper SSL**. La connessione supporta il gateway Juniper Networks SSL VPN, serie SA, versione 6.4 o successiva con il pacchetto Juniper Networks IVE versione 7.0 o successiva. Per configurare la connessione VPN, installare l'app JUNOS dall'App Store nel dispositivo mobile MDM iOS.

   - **F5 SSL**. La connessione supporta le soluzioni F5 BIG-IP Edge Gateway, Access Policy Manager e Fire SSL VPN. Per configurare la connessione VPN, installare l'app F5 BIG-IP Edge Client dall'App Store nel dispositivo mobile MDM iOS.

   - **SonicWALL Mobile Connect**. La connessione supporta i dispositivi SonicWALL Aventail E-Class Secure Remote Access versione 10.5.4 o successiva, i dispositivi SonicWALL SRA versione 5.5 o successiva, nonché i dispositivi SonicWALL Next-Generation Firewall, inclusi TZ, NSA, E-Class NSA con SonicOS versione 5.8.1.0 o successiva. Per configurare la connessione VPN, installare l'app SonicWALL Mobile Connect dall'App Store nel dispositivo mobile MDM iOS.

   - **Aruba VIA**. La connessione supporta i controller di accesso mobile Aruba Networks. Per configurarli, installare l'app Aruba Networks VIA dall'App Store nel dispositivo mobile MDM iOS.

   - **SSL personalizzato**. La connessione supporta l'autenticazione dell'utente del dispositivo mobile MDM iOS tramite password e certificati e autenticazione a due fattori.

8. Nel campo **Indirizzo server** immettere il nome di rete o l'indirizzo IP del server VPN.

9. Nel campo **Nome account** immettere il nome dell'account per l'autorizzazione nel server VPN. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

10. Configurare le impostazioni di sicurezza per la connessione VPN in base al tipo selezionato di rete privata virtuale.

11. Se necessario, configurare le impostazioni della connessione VPN tramite un server proxy:

    a. Selezionare la scheda **Impostazioni del server proxy**.

    b. Selezionare la modalità di configurazione del server proxy e specificare le impostazioni di connessione.

c. Fare clic su **OK**.

Come risultato, le impostazioni di connessione del dispositivo a una VPN tramite un server proxy vengono configurate nel dispositivo MDM iOS.

12. Fare clic su **OK**.

    La nuova VPN viene visualizzata nell'elenco.

13. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, una connessione VPN sarà configurata nel dispositivo MDM iOS dell'utente.

Configurazione del firewall nei dispositivi Android (solo Samsung)

Configurare le impostazioni del firewall per monitorare le connessioni di rete nel dispositivo mobile dell'utente.

Per configurare il firewall in un dispositivo mobile:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Gestisci Samsung KNOX → Gestisci dispositivo Samsung**.
5. Nella finestra **Firewall** fare clic su **Configura**.

   Verrà visualizzata la finestra **Firewall**.
6. Selezionare la modalità Firewall:
   - Per consentire tutte le connessioni in entrata e in uscita, spostare il cursore su **Consenti tutto**.
   - Per bloccare tutte le attività di rete tranne quelle delle app nell'elenco delle esclusioni, spostare il cursore su **Blocca tutto tranne le eccezioni**.
7. Se è stata impostata la modalità Firewall su **Blocca tutto tranne le eccezioni**, creare un elenco di esclusioni:
   a. Fare clic su **Aggiungi**.

      Verrà visualizzata la finestra **Esclusione per Firewall**.

   b. Nel campo **Nome app** immettere il nome di un'app mobile.

   c. Nel campo **Nome pacchetto** immettere il nome di sistema del pacchetto di app mobili (ad esempio `com.mobileapp.example`).

   d. Fare clic su **OK**.
8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Protezione di Kaspersky Endpoint Security for Android dalla rimozione

Per la protezione dei dispositivi mobili e la conformità con i requisiti di sicurezza aziendali, è possibile abilitare la protezione dalla rimozione di Kaspersky Endpoint Security for Android. In questo caso, l'utente non può rimuovere l'app utilizzando l'interfaccia di Kaspersky Endpoint Security for Android. Durante la rimozione dell'app tramite gli strumenti del sistema operativo Android, viene richiesto di disabilitare i diritti di amministratore per Kaspersky Endpoint Security for Android. Dopo aver disabilitato i diritti, il dispositivo mobile verrà bloccato.

In alcuni dispositivi Samsung con Android 7.0 o versioni successive, quando l'utente tenta di configurare metodi non supportati per lo sblocco del dispositivo (ad esempio, una password grafica), il dispositivo può essere bloccato se vengono soddisfatte le seguenti condizioni: la protezione dalla rimozione di Kaspersky Endpoint Security for Android è abilitata e sono impostati requisiti per la complessità della password di sblocco dello schermo. Per sbloccare il dispositivo, è necessario inviare un comando speciale al dispositivo.

Per abilitare la protezione dalla rimozione di Kaspersky Endpoint Security for Android:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Avanzate**.
5. Nella sezione **Rimozione di Kaspersky Endpoint Security for Android** deselezionare la casella **Consenti la rimozione di Kaspersky Endpoint Security for Android**.

   Per proteggere l'app dalla rimozione nei dispositivi che eseguono Android 7.0 o versioni successive, Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Durante l'esecuzione della procedura guidata di configurazione iniziale, Kaspersky Endpoint Security for Android richiede all'utente di concedere all'applicazione tutte le autorizzazioni richieste. L'utente può ignorare questi passaggi o disabilitare tali autorizzazioni nelle impostazioni del dispositivo in un momento successivo. In tal caso, l'app non è protetta dalla rimozione.

6. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. Se viene effettuato un tentativo di rimozione dell'app, il dispositivo mobile verrà bloccato.

Rilevamento delle manomissioni dei dispositivi (root)

Kaspersky Security for Mobile consente di rilevare le manomissioni dei dispositivi (root). In un dispositivo manomesso i file di sistema non sono protetti e quindi possono essere modificati. Inoltre, nei dispositivi manomessi possono essere installate app di terze parti da origini sconosciute. Al rilevamento di un tentativo di manomissione, è consigliabile ripristinare immediatamente il normale funzionamento del dispositivo.

Per rilevare quando un utente ottiene i privilegi di root, Kaspersky Endpoint Security for Android utilizza i seguenti servizi:

- *Servizio integrato di Kaspersky Endpoint Security for Android* è un servizio di Kaspersky che verifica se l'utente di un dispositivo mobile ha ottenuto privilegi di root (Kaspersky Mobile Security SDK).
- *Attestazione SafetyNet* è un servizio di Google che controlla l'integrità del sistema operativo, analizza l'hardware e il software del dispositivo e identifica altri problemi di sicurezza. Per maggiori informazioni sull'attestazione SafetyNet, visitare il sito Web dell'assistenza tecnica di Android.

Se un dispositivo è risulta manomesso, l'utente riceve una notifica. È possibile visualizzare le notifiche sulle manomissioni nell'area di lavoro di Administration Server nella scheda **Monitoraggio**. È inoltre possibile disabilitare le notifiche delle manomissioni nelle impostazioni di notifica degli eventi.

Nei dispositivi Android è possibile imporre restrizioni sull'attività dell'utente nel dispositivo se questo risulta manomesso (ad esempio, il blocco del dispositivo). È possibile imporre restrizioni utilizzando il componente Controllo conformità (vedere la figura seguente). A tale scopo, nelle impostazioni delle regole di scansione selezionare il criterio **Il dispositivo è stato dotato dell'accesso root**.

Configurazione di un proxy di HTTP globale nei dispositivi MDM iOS

Per proteggere il traffico Internet dell'utente, configurare la connessione a Internet del dispositivo MDM iOS tramite un server proxy.

La connessione automatica a Internet tramite un server proxy è disponibile solo per i dispositivi controllati.

Per configurare le impostazioni del proxy HTTP globale nel dispositivo MDM iOS dell'utente:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Proxy HTTP globale**.
5. Nella sezione **Impostazioni proxy HTTP globale** selezionare la casella **Applica impostazioni nel dispositivo**.
6. Selezionare il tipo di configurazione del proxy HTTP globale.

   Per impostazione predefinita, è selezionato il tipo di configurazione manuale del proxy HTTP globale e l'utente non può eseguire la connessione a reti captive senza eseguire la connessione a un server proxy. Le *reti captive* sono reti wireless che richiedono l'autenticazione preliminare nel dispositivo mobile senza la connessione al server proxy.

   - Per specificare manualmente le impostazioni di connessione al server proxy:
     a. Nell'elenco a discesa **Tipo di impostazioni proxy** selezionare **Manuale**.
     b. Nel campo **Porta e indirizzo server proxy** immettere il nome di un host o l'indirizzo IP di un server proxy e il numero della porta del server proxy.

c. Nel campo **Nome utente** immettere il nome dell'account utente per l'autorizzazione del server proxy. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

d. Nel campo **Password** immettere la password dell'account per l'autorizzazione del server proxy.

e. Per consentire all'utente di accedere alle reti captive, selezionare la casella **Consenti l'accesso alle reti captive senza la connessione al proxy**.

- Per configurare le impostazioni di connessione al server proxy utilizzando un file PAC (Proxy Auto Configuration):

a. Nell'elenco a discesa **Tipo di impostazioni proxy** selezionare **Automatica**.

b. Nel campo **URL del file PAC** immettere l'indirizzo Web del file PAC (ad esempio, http://www.esempio.com/nomefile.pac).

c. Per consentire all'utente di connettere il dispositivo mobile a una rete wireless senza utilizzare un server proxy quando non è possibile accedere al file PAC, selezionare la casella **Consenti connessione diretta se non è possibile accedere al file PAC**.

d. Per consentire all'utente di accedere alle reti captive, selezionare la casella **Consenti l'accesso alle reti captive senza la connessione al proxy**.

7. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, l'utente del dispositivo mobile si connetterà a Internet tramite un server proxy.

Aggiunta dei certificati di sicurezza ai dispositivi MDM iOS

Per semplificare l'autenticazione dell'utente e garantire la protezione dei dati, aggiungere certificati nel dispositivo MDM iOS dell'utente. I dati firmati con un certificato sono protetti dalla modifica durante lo scambio in rete. Il criptaggio dei dati tramite un certificato fornisce un livello aggiuntivo di sicurezza per i dati. Il certificato può inoltre essere utilizzato per la verifica dell'identità dell'utente.

Kaspersky Device Management for iOS supporta i seguenti standard per i certificati:

- **PKCS#1** – criptaggio con una chiave pubblica basata sugli algoritmi RSA.
- **PKCS#12** – archiviazione e trasmissione di un certificato e una chiave privata.

Per aggiungere un certificato di sicurezza nel dispositivo MDM iOS di un utente:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** selezionare la sezione **Certificati**.
5. Fare clic sul pulsante **Aggiungi** nella sezione **Certificati**.

   Verrà visualizzata la finestra **Certificato**.

6. Nel campo **Nome file** specificare il percorso del certificato:

   I file dei certificati PKCS#1 hanno estensioni cer, crt o der. I file dei certificati PKCS#12 hanno estensioni p12 o pfx.

7. Fare clic su **Apri**.

   Se il certificato è protetto tramite password, specificare la password. Il nuovo certificato viene visualizzato nell'elenco.

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, all'utente verrà richiesto di installare i certificati inseriti nell'elenco creato.

Aggiunta di un profilo SCEP ai dispositivi MDM iOS

È necessario aggiungere un profilo SCEP per consentire all'utente del dispositivo MDM iOS di ricevere automaticamente i certificati dal centro di certificazione via Internet. Il profilo SCEP fornisce il supporto per il protocollo Simple Certificate Enrollment Protocol.

Per impostazione predefinita, viene aggiunto un profilo SCEP con le seguenti impostazioni:

- Il nome alternativo dell'oggetto non viene utilizzato per la registrazione dei certificati.
- Vengono effettuati tre tentativi di polling del server SCEP a distanza di 10 secondi. Se tutti i tentativi di firmare il certificato hanno esito negativo, è necessario generare una nuova richiesta di firma del certificato.
- Il certificato ricevuto non può essere utilizzato per la firma o il criptaggio dei dati.

È possibile modificare le impostazioni specificate durante l'aggiunta del profilo SCEP.

Per aggiungere un profilo SCEP:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **SCEP**.
5. Fare clic sul pulsante **Aggiungi** nella sezione **Profili SCEP**.

   Verrà visualizzata la finestra **Profilo SCEP**.

6. Nel campo **Indirizzo Web server** immettere l'indirizzo Web del server SCEP in cui è distribuito il centro di certificazione.

   L'URL può contenere l'indirizzo IP o il nome di dominio completo (FQDN). Ad esempio: http://10.10.10.10/servercert/scepazienda.

7. Nel campo **Nome** immettere il nome del centro di certificazione distribuito nel server SCEP.

8. Nel campo **Oggetto** immettere una stringa con gli attributi dell'utente del dispositivo MDM iOS che sono contenuti nel certificato X.500.

   Gli attributi possono contenere i dettagli sul paese (C), l'organizzazione (O) e il nome comune dell'utente (CN). Ad esempio: /C=IT/O=Azienda/CN=Utente/. È anche possibile utilizzare gli altri attributi specificati nella specifica RFC 5280.

9. Nell'elenco a discesa **Tipo di nome alternativo dell'oggetto** selezionare il tipo di nome alternativo dell'oggetto del server SCEP:

   - **No** – l'identificazione tramite nome alternativo non viene utilizzata.
   - **Nome RFC 822** – identificazione tramite l'indirizzo e-mail. L'indirizzo e-mail deve essere specificato in base alla specifica RFC 822.
   - **Nome DNS** – identificazione tramite nome di dominio.
   - **URI** – identificazione tramite indirizzo IP o indirizzo in formato FQDN.

   È possibile utilizzare un nome alternativo dell'oggetto per identificare l'utente del dispositivo mobile MDM iOS.

10. Nel campo **Nome alternativo dell'oggetto** immettere il nome alternativo dell'oggetto del certificato X.500. Il valore del nome alternativo dell'oggetto dipende dal tipo di oggetto: indirizzo e-mail dell'utente, dominio o indirizzo Web.

11. Nel campo **Nome dell'oggetto NT** immettere il nome DNS dell'utente del dispositivo mobile MDM iOS nella rete Windows NT.

    Il nome dell'oggetto NT è contenuto nella richiesta di certificato inviata al server SCEP.

12. Nel campo **Numero di tentativi di polling nel server SCEP** specificare il numero massimo di tentativi di polling del server SCEP per ottenere il certificato firmato.

13. Nel campo **Frequenza dei tentativi (sec)** specificare il periodo di tempo in secondi tra i tentativi di polling del server SCEP per ottenere il certificato firmato.

14. Nel campo **Richiesta di registrazione** immettere una chiave di registrazione prepubblicata.

    Prima di firmare un certificato, il server SCEP richiede all'utente del dispositivo mobile di specificare una chiave. Se questo campo viene lasciato vuoto, il server SCEP non richiede la chiave.

15. Nell'elenco a discesa **Dimensioni chiave** selezionare la dimensione della chiave di registrazione in bit: 1024 o 2048.

16. Se si desidera consentire all'utente di utilizzare un certificato ricevuto dal server SCEP come certificato di firma, selezionare la casella **Usa per la firma**.

17. Se si desidera consentire all'utente di utilizzare un certificato ricevuto dal server SCEP per il criptaggio dei dati, selezionare la casella **Usa per il criptaggio**.

    Non è consentito utilizzare il certificato del server SCEP come certificato di firma e certificato di criptaggio dei dati contemporaneamente.

18. Nel campo **Impronta digitale del certificato** immettere l'impronta digitale univoca del certificato per la verifica dell'autenticità della risposta dal centro di certificazione. È possibile utilizzare le impronte digitali dei certificati con l'algoritmo di hashing SHA-1 o MD5. È possibile copiare manualmente l'impronta digitale del certificato o selezionare un certificato utilizzando il pulsante **Crea a partire dal certificato**. Quando si crea l'impronta

digitale utilizzando il pulsante **Crea a partire dal certificato**, l'impronta digitale viene aggiunta automaticamente al campo.

> È necessario specificare l'impronta digitale del certificato se lo scambio dei dati tra il dispositivo mobile e il centro di certificazione avviene tramite il protocollo HTTP.

19. Fare clic su **OK**.

    Il nuovo profilo SCEP viene visualizzato nell'elenco.

20. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, il dispositivo mobile dell'utente è configurato per ricevere automaticamente un certificato dal centro di certificazione via Internet.

Controllo

Questa sezione contiene informazioni su come monitorare in remoto i dispositivi mobili in Administration Console di Kaspersky Security Center.

Configurazione delle restrizioni

Questa sezione offre istruzioni su come configurare l'accesso dell'utente alle funzionalità dei dispositivi mobili.

Considerazioni speciali per i dispositivi che eseguono Android versione 10 e successive

Android 10 ha introdotto numerose modifiche e limitazioni relative all'API 29 o versioni successive. Alcune di queste modifiche influiscono sulla disponibilità o sul funzionamento di alcune funzionalità dell'app. Queste considerazioni si applicano solo ai dispositivi che eseguono Android 10 o versioni successive.

Possibilità di abilitare, disabilitare e configurare il Wi-Fi

- Le reti Wi-Fi possono essere aggiunte, eliminate e configurate in Administration Console di Kaspersky Security Center. Quando una rete Wi-Fi viene aggiunta a un criterio, Kaspersky Endpoint Security riceve questa configurazione di rete al momento della prima connessione a Kaspersky Security Center.
- Quando un dispositivo rileva una rete configurata tramite Kaspersky Security Center, Kaspersky Endpoint Security richiede all'utente di connettersi a tale rete. Se l'utente sceglie di connettersi alla rete, tutte le impostazioni configurate tramite Kaspersky Security Center vengono applicate automaticamente. Il dispositivo si connette quindi automaticamente alla rete quando si trova nel raggio d'azione, senza mostrare ulteriori notifiche all'utente.
- Se il dispositivo di un utente è già connesso a un'altra rete Wi-Fi, a volte all'utente potrebbe non essere richiesto di approvare l'aggiunta di una rete. In questi casi l'utente deve spegnere e riaccendere il Wi-Fi per ricevere il suggerimento.
- Quando Kaspersky Endpoint Security suggerisce a un utente di connettersi a una rete Wi-Fi e l'utente rifiuta di farlo, l'autorizzazione dell'app per modificare lo stato del Wi-Fi viene revocata. Kaspersky Endpoint Security non

può quindi suggerire di connettersi alle reti Wi-Fi finché l'utente non concede nuovamente l'autorizzazione accedendo a **Impostazioni → App e notifiche → Accesso speciale all'app → Controllo Wi-Fi → Kaspersky Endpoint Security**.

- Sono supportate solo reti aperte e reti criptate con WPA2-PSK. I tipi di criptaggio WEP e WPA non sono supportati.
- Se la password per una rete precedentemente suggerita dall'app viene modificata, l'utente deve eliminare manualmente tale rete dall'elenco delle reti note. Il dispositivo sarà quindi in grado di ricevere un suggerimento di rete da Kaspersky Endpoint Security e connettersi.
- Quando il sistema operativo di un dispositivo viene aggiornato da Android versione 9 o precedente ad Android versione 10 o successiva e/o viene aggiornato Kaspersky Endpoint Security installato in un dispositivo che esegue Android versione 10 o successiva, le reti precedentemente aggiunte tramite Kaspersky Security Center non possono essere modificate o eliminate tramite i criteri di Kaspersky Security Center. L'utente può tuttavia modificare o eliminare manualmente tali reti nelle impostazioni del dispositivo.
- Nei dispositivi che eseguono Android 10 all'utente viene richiesta la password durante un tentativo di connessione manuale a una rete consigliata protetta. La connessione automatica non richiede l'immissione della password. Se il dispositivo di un utente è connesso a un'altra rete Wi-Fi, l'utente deve prima disconnettersi da tale rete per connettersi automaticamente a una delle reti suggerite.
- Nei dispositivi che eseguono Android 11 un utente può connettersi manualmente a una rete protetta suggerita dall'app senza inserire la password.
- Quando Kaspersky Endpoint Security viene rimosso da un dispositivo, le reti suggerite in precedenza dall'app vengono ignorate.
- Il divieto di utilizzare le reti Wi-Fi non è supportato.

Accesso alla fotocamera

- Nei dispositivi che eseguono Android 10 l'utilizzo della fotocamera non può essere completamente vietato. Il divieto di utilizzare la fotocamera per un profilo lavoro è comunque disponibile.
- Se un'app di terze parti tenta di accedere alla fotocamera del dispositivo, l'app verrà bloccata e l'utente riceverà una notifica sul problema. Tuttavia, le app che utilizzano la fotocamera durante l'esecuzione in background non possono essere bloccate.
- Quando una fotocamera esterna viene scollegata da un dispositivo, in alcuni casi potrebbe essere visualizzata una notifica relativa alla mancata disponibilità della fotocamera.

Gestione dei metodi di sblocco dello schermo

- Kaspersky Endpoint Security adesso risolve i requisiti di complessità della password in uno dei valori di sistema: medio o alto.
  - Se la lunghezza della password richiesta è compresa tra 1 e 4 simboli, l'app richiede all'utente di impostare una password di complessità media. Deve essere una password numerica (PIN) senza sequenze ripetute o ordinate (ad es. 1234) oppure alfanumerica. Il PIN o la password deve contenere almeno 4 caratteri.
  - Se la lunghezza della password richiesta è superiore a 5 simboli, l'app richiede all'utente di impostare una password di complessità alta. Deve essere una password numerica (PIN) senza sequenze ripetute o ordinate oppure alfanumerica (password). Il PIN deve contenere almeno 8 cifre; la password deve contenere almeno 6 caratteri.

- L'uso dell'impronta digitale per sbloccare lo schermo può essere gestito solo per un profilo lavoro.

Configurazione delle restrizioni per i dispositivi Android

Per garantire la protezione di un dispositivo Android, configurare le impostazioni di utilizzo del Wi-Fi, della fotocamera e del Bluetooth nel dispositivo.

Per impostazione predefinita, l'utente può utilizzare il Wi-Fi, la fotocamera e il Bluetooth nel dispositivo senza restrizioni.

Per configurare le restrizioni di utilizzo del Wi-Fi, della fotocamera e del Bluetooth nel dispositivo:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Gestione dispositivo**.
5. Nella sezione **Restrizioni** configurare l'utilizzo del Wi-Fi, della fotocamera e della connettività Bluetooth:
   - Per disabilitare il modulo Wi-Fi nel dispositivo mobile dell'utente, selezionare la casella **Impedisci l'uso del Wi-Fi**.

     Nei dispositivi con Android 10.0 o versioni successive, il divieto di utilizzo delle reti Wi-Fi non è supportato.

   - Per disabilitare la fotocamera nel dispositivo mobile dell'utente, selezionare la casella **Impedisci l'uso della fotocamera**.

     Nei dispositivi che eseguono Android 10.0 o versioni successive, l'utilizzo della fotocamera non può essere completamente vietato.

     Nei dispositivi che eseguono Android 11 o versioni successive Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo. In tal caso, non sarà possibile limitare l'utilizzo della fotocamera.

   - Per disabilitare la connettività Bluetooth nel dispositivo mobile dell'utente, selezionare la casella **Impedisci l'uso del Bluetooth**.

     In Android 12 o versioni successive l'utilizzo del Bluetooth può essere disabilitato solo se l'utente del dispositivo ha concesso l'autorizzazione **Dispositivi Bluetooth nelle vicinanze**. L'utente può concedere questa autorizzazione durante la procedura guidata di configurazione iniziale o in un secondo momento.

6. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione delle restrizioni per le funzionalità dei dispositivi MDM iOS

Per assicurare la conformità ai requisiti di sicurezza aziendali, configurare restrizioni per l'esecuzione del dispositivo MDM iOS.

Per configurare restrizioni per le funzionalità dei dispositivi MDM iOS:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Restrizione per le funzionalità**.
5. Nella sezione **Impostazioni delle restrizioni per le funzionalità** selezionare la casella **Applica impostazioni nel dispositivo**.
6. Configurare le restrizioni per le funzionalità dei dispositivi MDM iOS.
7. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.
8. Selezionare la sezione **Restrizioni per le applicazioni**.
9. Nella sezione **Impostazioni delle restrizioni per le applicazioni** selezionare la casella **Applica impostazioni nel dispositivo**.
10. Configurare le restrizioni per le app nel dispositivo MDM iOS.
11. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.
12. Selezionare la sezione **Limitazioni per i contenuti multimediali**.
13. Nella sezione **Impostazioni di limitazione dei contenuti multimediali** selezionare la casella **Applica impostazioni nel dispositivo**.
14. Configurare le restrizioni per i contenuti multimediali nel dispositivo MDM iOS.
15. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, le restrizioni per le funzionalità, le app e i contenuti multimediali verranno configurate nel dispositivo mobile dell'utente.

Configurazione delle restrizioni per le funzionalità dei dispositivi EAS

Configurare restrizioni per le funzionalità del dispositivo per mantenere protetto un dispositivo EAS.

Per impostazione predefinita, l'utente può utilizzare le funzionalità di un dispositivo EAS senza restrizioni.

Per configurare restrizioni per le funzionalità dei dispositivi EAS:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi EAS.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra Proprietà del criterio selezionare la sezione **Restrizione per le funzionalità**.
5. Nella sezione **Impostazioni delle restrizioni per le funzionalità** consentire o bloccare l'utilizzo delle funzionalità del dispositivo EAS:
   - Per consentire la connessione di schede di memoria e altre unità rimovibili al dispositivo, selezionare la casella **Consenti unità rimovibili**.
   - Per consentire l'utilizzo della fotocamera, selezionare la casella **Consenti utilizzo della fotocamera**.
   - Per consentire le connessioni Wi-Fi, selezionare la casella **Consenti utilizzo del Wi-Fi**.
   - Per consentire l'utilizzo della porta di connessione a infrarossi, selezionare **Consenti connessione a infrarossi**.
   - Per consentire l'utilizzo del dispositivo come un punto di accesso Wi-Fi per la creazione di una rete wireless, selezionare la casella **Consenti l'utilizzo del dispositivo come punto di accesso Wi-Fi**.
   - Per consentire al dispositivo di connettersi a un desktop remoto, selezionare la casella **Consenti connessione Desktop remoto**.
   - Per consentire l'utilizzo del client desktop ActiveSync nel dispositivo, selezionare la casella **Consenti sincronizzazione desktop**.
   - Nell'elenco a discesa **Utilizzo del Bluetooth** consentire o bloccare l'utilizzo del Bluetooth nel dispositivo EAS:
     - **Consenti**. L'utilizzo del Bluetooth nel dispositivo mobile è consentito.
     - **Quando si utilizza il viva voce**. L'utilizzo del Bluetooth è consentito quando viene connesso un auricolare wireless al dispositivo mobile.
     - **Nega**. L'utilizzo del Bluetooth nel dispositivo mobile è bloccato.
6. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione dell'accesso dell'utente ai siti Web

Questa sezione contiene istruzioni su come configurare l'accesso ai siti Web nei dispositivi iOS e Android.

Configurazione dell'accesso ai siti Web nei dispositivi Android

È possibile utilizzare Protezione Web per configurare l'accesso ai siti Web degli utenti dei dispositivi Android. Protezione Web supporta il filtro dei siti Web in base alle categorie definite nel servizio cloud Kaspersky Security Network. Il filtro consente di limitare l'accesso degli utenti a determinati siti Web o categorie di siti Web (ad esempio, quelli delle categorie "Gioco d'azzardo, lotterie, scommesse" o "Comunicazioni di rete"). Protezione Web protegge inoltre i dati personali degli utenti su Internet.

Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo. In questo caso, Protezione Web non verrà eseguito.

Protezione Web nei dispositivi Android funziona solo nel browser Google Chrome (inclusa la funzionalità Schede personalizzate), in Huawei Browser e Samsung Internet Browser. Protezione Web per Samsung Internet Browser non blocca i siti su un dispositivo mobile se viene utilizzato un profilo lavoro e Protezione Web è abilitato solo per il profilo lavoro.

Protezione Web è abilitato per impostazione predefinita: l'accesso dell'utente ai siti Web nelle categorie **Phishing** e **Malware** è bloccato.

Per configurare le impostazioni per l'accesso dell'utente del dispositivo ai siti Web:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare **Protezione Web**.
5. Selezionare la casella **Abilita Protezione Web**.
6. Per utilizzare Protezione Web, l'utente o l'utente del dispositivo deve leggere e accettare l'Informativa relativa all'elaborazione dei dati a scopo di utilizzo di Protezione Web (Informativa di Protezione Web):
   a. Fare clic sul collegamento **Informativa di Protezione Web**.

      Viene visualizzata la finestra **Informativa relativa all'elaborazione dei dati a scopo di utilizzo di Protezione Web**. Per accettare l'Informativa di Protezione Web, è necessario leggere e accettare l'Informativa sulla privacy.

   b. Fare clic sul collegamento dell'Informativa sulla privacy. Leggere e accettare l'Informativa sulla privacy.

      Se non si accetta l'Informativa sulla privacy, l'utente del dispositivo mobile può accettare l'Informativa sulla privacy nella Configurazione iniziale guidata o nell'app (→ **Informazioni sull'app** → **Termini e condizioni** → **Informativa sulla privacy**).

   c. Selezionare la modalità di accettazione dell'Informativa di Protezione Web:
      - **Ho letto e accetto l'Informativa di Protezione Web**
      - **Richiedi l'accettazione dell'Informativa di Protezione Web da parte dell'utente del dispositivo**
      - **Non accetto l'Informativa di Protezione Web**

Se si seleziona **Non accetto l'Informativa di Protezione Web**, Protezione Web non blocca i siti in un dispositivo mobile. L'utente del dispositivo mobile non può abilitare Protezione Web in Kaspersky Endpoint Security.

7. Se si desidera che l'app limiti l'accesso dell'utente ai siti Web a seconda del relativo contenuto, eseguire le seguenti operazioni:

   a. Nella sezione **Protezione Web**, nell'elenco a discesa selezionare **I siti Web delle categorie selezionate sono vietati**.

   b. Creare un elenco di categorie bloccate selezionando le caselle di controllo accanto alle categorie di siti Web alle quali l'app bloccherà l'accesso.

8. Se si desidera che l'app consenta l'accesso dell'utente solo ai siti Web specificati dall'amministratore, eseguire le seguenti operazioni:

   a. Nella sezione **Protezione Web**, nell'elenco a discesa selezionare **Solo i siti Web elencati sono consentiti**.

   b. Creare un elenco di siti Web aggiungendo gli indirizzi dei siti Web ai quali l'app non bloccherà l'accesso. Kaspersky Endpoint Security for Android supporta solo espressioni regolari. Durante l'immissione dell'indirizzo di un sito Web consentito, utilizzare i seguenti modelli:

      - `http:\/\/www\.example\.com.*`: tutte le pagine secondarie dei siti Web sono consentite (ad esempio `http://www.example.com/about`).

      - `https:\/\/.*example\.com`: tutte le pagine del sottodominio del sito Web sono consentite (ad esempio `https://pictures.example.com`).

      È inoltre possibile utilizzare l'espressione `https?` per selezionare i protocolli HTTP e HTTPS. Per maggiori informazioni sulle espressioni regolari, fare riferimento al sito Web dell'assistenza tecnica di Oracle.

9. Se si desidera che l'app blocchi l'accesso dell'utente a tutti i siti Web, nell'elenco a discesa della sezione **Protezione Web** selezionare **Tutti i siti Web sono bloccati**.

10. Per applicare restrizioni basate sul contenuto per l'accesso dell'utente, selezionare la casella **Abilita Protezione Web**.

11. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione dell'accesso ai siti Web nei dispositivi MDM iOS

Configurare le impostazioni di Protezione Web per controllare l'accesso ai siti Web per gli utenti dei dispositivi MDM iOS. Protezione Web controlla l'accesso di un utente ai siti Web in base agli elenchi di siti Web consentiti e bloccati. Protezione Web consente inoltre di aggiungere segnalibri ai siti Web nel pannello dei segnalibri in Safari.

Per impostazione predefinita, non vengono applicate restrizioni per l'accesso ai siti Web.

È possibile configurare le impostazioni di Protezione Web solo per i dispositivi supervisionati.

Per configurare l'accesso ai siti Web nel dispositivo MDM iOS dell'utente:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic.

4. Nella finestra **Proprietà** del criterio selezionare **Protezione Web**.

5. Nella sezione **Impostazioni di Protezione Web** selezionare la casella **Applica impostazioni nel dispositivo**.

6. Per bloccare l'accesso ai siti Web bloccati e consentire l'accesso ai siti Web consentiti:

   a. Nell'elenco a discesa **Modalità Filtro Web** selezionare la modalità **Limita contenuti per adulti**.

   b. Nella sezione **Siti Web consentiti** creare un elenco di siti Web consentiti.

      L'indirizzo del sito Web deve iniziare con `"http://"` o `"https://"`. Kaspersky Device Management for iOS consente l'accesso a tutti i siti Web nel dominio. Ad esempio, se è stato aggiunto http://www.example.com all'elenco dei siti Web consentiti, l'accesso è consentito a http://pictures.example.com e http://example.com/movies. Se l'elenco dei siti Web consentiti è vuoto, l'applicazione consente l'accesso a tutti i siti Web diversi da quelli inclusi nell'elenco dei siti Web bloccati.

   c. Nella sezione **Siti Web vietati** creare un elenco di siti Web bloccati.

      L'indirizzo del sito Web deve iniziare con `"http://"` o `"https://"`. Kaspersky Device Management for iOS blocca l'accesso a tutti i siti Web nel dominio.

7. Per bloccare l'accesso a tutti i siti Web diversi da quelli consentiti nell'elenco della scheda:

   a. Nell'elenco a discesa **Modalità Filtro Web** selezionare la modalità **Consenti solo i siti Web aggiunti ai segnalibri**.

   b. Nella sezione **Segnalibri** creare un elenco di segnalibri di siti Web consentiti.

      L'indirizzo del sito Web deve iniziare con `"http://"` o `"https://"`. Kaspersky Device Management for iOS consente l'accesso a tutti i siti Web nel dominio. Se l'elenco dei segnalibri è vuoto, l'applicazione consente l'accesso a tutti i siti Web. Kaspersky Management for iOS aggiunge i siti Web nell'elenco dei segnalibri nella scheda Segnalibri di Safari nel dispositivo mobile dell'utente.

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, il componente Protezione Web verrà configurato nel dispositivo mobile dell'utente in base alla modalità selezionata e agli elenchi creati.

Controllo conformità dei dispositivi Android con i requisiti di sicurezza aziendali

È possibile verificare la conformità dei dispositivi Android con i requisiti di sicurezza aziendali. I requisiti di sicurezza aziendali definiscono il modo in cui l'utente può utilizzare il dispositivo. Ad esempio, la protezione in tempo reale deve essere abilitata nel dispositivo, i database anti-virus devono essere aggiornati e la password del dispositivo deve essere sufficientemente complessa. Controllo conformità si basa su un elenco di regole. Una regola di conformità include i seguenti componenti:

- Criterio di controllo del dispositivo (ad esempio, l'assenza di app bloccate nel dispositivo).

- Periodo di tempo assegnato all'utente per correggere la mancata conformità (ad esempio, 24 ore).

- Azione che verrà eseguita nel dispositivo se l'utente non corregge la mancata conformità entro il periodo di tempo definito (ad esempio, il blocco del dispositivo).

  In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

Se l'utente non risolve l'inadempienza entro il periodo di tempo specificato, sono disponibili le azioni seguenti:

- **Blocca tutte le applicazioni eccetto quelle di sistema**. L'avvio di tutte le app nel dispositivo mobile dell'utente, ad eccezione di quelle di sistema, è bloccato.

- **Blocca dispositivo**. Il dispositivo mobile è bloccato. Per ottenere l'accesso ai dati, è necessario sbloccare il dispositivo. Se il motivo del blocco del dispositivo non viene rettificato dopo lo sblocco del dispositivo, il dispositivo verrà bloccato nuovamente dopo il periodo di tempo specificato.

- **Cancella dati aziendali**. Cancellare i dati inseriti in un contenitore, account e-mail aziendale, impostazioni per la connessione alla rete Wi-Fi aziendale e alla VPN, nome del punto di accesso (APN), profilo lavoro Android, contenitore KNOX e chiave di gestione delle licenze KNOX.

- **Reset Dispositivo**. Tutti i dati vengono eliminati dal dispositivo mobile e viene eseguito il rollback delle impostazioni ai valori predefiniti. Dopo il completamento di questa azione, il dispositivo non sarà più un dispositivo gestito. Per collegare il dispositivo a Kaspersky Security Center, è necessario reinstallare Kaspersky Endpoint Security for Android.

Per creare una regola di scansione per la verifica della conformità dei dispositivi a un criterio di gruppo:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Controllo conformità**.

5. Per ricevere notifiche sui dispositivi non conformi al criterio, nella sezione **Notifica sulla mancata conformità** selezionare la casella **Notifica all'amministratore**.

   Se il dispositivo non è conforme a un criterio, durante la sincronizzazione del dispositivo con Administration Server, Kaspersky Endpoint Security for Android scrive una voce relativa a **Violazione rilevata: <nome del criterio controllato>** nel registro eventi. È possibile visualizzare il Registro eventi nella scheda **Eventi** nelle proprietà di Administration Server o nelle proprietà locali dell'applicazione.

6. Per notificare all'utente del dispositivo che il dispositivo non è conforme al criterio, nella sezione **Notifica sulla mancata conformità** selezionare la casella **Notifica all'utente**.

   Se il dispositivo non è conforme a un criterio, durante la sincronizzazione del dispositivo con l'Administration Server, Kaspersky Endpoint Security for Android notifica il problema all'utente nella sezione **Stato**.

7. Nella sezione **Regole di conformità** compilare un elenco di regole per la verifica della conformità del dispositivo al criterio. Eseguire le seguenti operazioni:

   a. Fare clic su **Aggiungi**.

      Verrà avviata la Procedura guidata regole di scansione.

   b. Seguire le istruzioni della Procedura guidata regole di scansione.

Al termine della procedura guidata, la nuova regola verrà visualizzata nella sezione **Regole di conformità** nell'elenco delle regole di scansione.

8. Per disabilitare temporaneamente una regola di scansione creata, utilizzare l'interruttore accanto alla regola selezionata.

9. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. Se il dispositivo dell'utente non è conforme alle regole, le restrizioni specificate nell'elenco delle regole di scansione vengono applicate al dispositivo.

Controllo dell'avvio delle app

Questa sezione contiene istruzioni su come configurare l'accesso dell'utente alle app in un dispositivo mobile.

Controllo dell'avvio delle app nei dispositivi Android

Per garantire la protezione del dispositivo mobile dell'utente, è necessario configurare le impostazioni per l'avvio delle app nel dispositivo.

È possibile imporre limitazioni all'attività dell'utente in un dispositivo nel quale sono installate app bloccate o le app obbligatorie non sono installate (ad esempio il blocco del dispositivo). È possibile imporre restrizioni utilizzando il componente Controllo conformità. A tale scopo, nelle impostazioni delle regole di scansione è necessario selezionare il criterio **App vietate installate**, **Installate app appartenenti alle categorie vietate** o **Non tutte le app obbligatorie sono installate**.

Kaspersky Endpoint Security for Android deve essere impostato come funzionalità di accessibilità al fine di garantire il corretto funzionamento di Controllo app. Kaspersky Endpoint Security for Android richiede all'utente di impostare l'app come funzionalità di accessibilità attraverso la procedura guidata di configurazione iniziale. L'utente può ignorare questo passaggio o disabilitare il servizio nelle impostazioni del dispositivo in un momento successivo. In questo caso, Controllo app non verrà eseguito.

Per configurare le impostazioni di avvio delle app nel dispositivo mobile:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Controllo app**.

5. Nella sezione **Modalità operativa** selezionare la modalità di avvio delle app nel dispositivo mobile dell'utente:

   - Per consentire all'utente di avviare tutte le app tranne quelle specificate nell'elenco delle categorie e delle app bloccate, selezionare la modalità **App bloccate**.

   - Per consentire all'utente di avviare solo le app specificate nell'elenco delle categorie e delle app consentite, consigliate o richieste, selezionare la modalità **App consentite**.

6. Se si desidera che Kaspersky Endpoint Security for Android invii dati sulle app vietate al registro eventi senza bloccarle, selezionare la casella di controllo **Non bloccare le app vietate, è sufficiente aggiungere un record al registro eventi**.

   Durante la successiva sincronizzazione del dispositivo mobile dell'utente con l'Administration Server, Kaspersky Endpoint Security for Android scrive una voce relativa a **È stata installata un'app vietata** nel registro eventi. È possibile visualizzare il Registro eventi nella scheda **Eventi** nelle proprietà di Administration Server o nelle proprietà locali dell'applicazione.

7. Se si desidera che Kaspersky Endpoint Security for Android blocchi l'avvio delle app di sistema nel dispositivo mobile dell'utente (ad esempio Calendario, Fotocamera e Impostazioni) nella modalità **App consentite**, selezionare la casella **Blocca app di sistema**.

   Gli esperti di Kaspersky consigliano di non bloccare le app di sistema poiché l'operazione potrebbe generare errori di funzionamento del dispositivo.

8. Creare un elenco di categorie e app per configurare l'avvio delle app.

   Per informazioni dettagliate sulle categorie di app, fare riferimento alle Appendici.

   Per un elenco delle app appartenenti a ogni categoria, visitare il sito Web di Kaspersky.

9. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione delle restrizioni dei dispositivo EAS per le applicazioni

Per mantenere protetto il dispositivo EAS, configurare le restrizioni per le attività delle applicazioni (browser, app prive di firma).

Per impostazione predefinita, l'utente può utilizzare le app in un dispositivo EAS senza restrizioni.

Per configurare le restrizioni per le attività delle applicazioni nel dispositivo EAS:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi EAS.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic.

4. Nella finestra Proprietà del criterio selezionare la sezione **Restrizioni per le applicazioni**.

5. Nella sezione **Impostazioni delle restrizioni per le applicazioni** configurare le restrizioni per le attività delle app:

   - Per consentire all'utente di utilizzare il browser, selezionare la casella **Consenti utilizzo del browser**.
   - Per consentire all'utente di creare account e-mail personali (POP3 o IMAP4), selezionare **Consenti posta personale**.
   - Per consentire all'utente di avviare le applicazioni che non sono state firmate con un certificato di autenticazione, selezionare la casella **Consenti applicazioni non firmate**.

- Per consentire all'utente di installare le applicazioni che non sono state firmate con un certificato di autenticazione, selezionare la casella **Consenti pacchetti di installazione non firmati**.

6. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Inventario software nei dispositivi Android

È possibile eseguire l'inventario delle app nei dispositivi Android connessi a Kaspersky Security Center. Kaspersky Endpoint Security for Android riceve le informazioni su tutte le app installate nei dispositivi mobili. Le informazioni acquisite durante l'inventario sono visualizzate nelle proprietà del dispositivo nella sezione **Eventi**. È possibile visualizzare informazioni dettagliate su ogni app installata, inclusi la versione e il produttore.

Per abilitare l'inventario software:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Controllo app**.

5. Nella sezione **Inventario software** selezionare la casella di controllo **Invia dati sulle app installate**.

6. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. Kaspersky Endpoint Security for Android invia i dati al registro eventi ogni volta che un'app viene installata o rimossa dal dispositivo.

Configurazione della visualizzazione dei dispositivi Android in Kaspersky Security Center

Per utilizzare al meglio l'elenco dei dispositivi mobili, è necessario configurare le impostazioni per la visualizzazione dei dispositivi in Kaspersky Security Center. Per impostazione predefinita, l'elenco dei dispositivi mobili è visualizzato nella struttura della console **Avanzate → Mobile Device Management → Dispositivi mobili**. Le informazioni sui dispositivi vengono aggiornate automaticamente. È inoltre possibile aggiornare manualmente l'elenco dei dispositivi mobili facendo clic sul pulsante **Aggiornamento** nell'angolo superiore destro.

Dopo la connessione del dispositivo a Kaspersky Security Center, i dispositivi vengono aggiunti automaticamente all'elenco dei dispositivi mobili. L'elenco dei dispositivi mobili potrebbe contenere informazioni dettagliate sul dispositivo: modello, sistema operativo, indirizzo IP e altro.

È possibile configurare il formato del nome del dispositivo e selezionare lo stato del dispositivo. Lo stato del dispositivo informa del funzionamento dei componenti di Kaspersky Endpoint Security for Android nel dispositivo mobile dell'utente.

I componenti di Kaspersky Endpoint Security for Android possono non funzionare per i seguenti motivi:

- L'utente ha disabilitato il componente nelle impostazioni del dispositivo.
- L'utente non ha concesso all'app le autorizzazioni necessarie per il funzionamento del componente (ad esempio, non è disponibile un'autorizzazione per determinare la posizione del dispositivo per il comando Antifurto corrispondente).

Per visualizzare lo stato del dispositivo, è necessario abilitare la condizione **Determinato dall'applicazione** nelle proprietà del gruppo di amministrazione (**Proprietà** → **Stato del dispositivo** → **Imposta stato del dispositivo su Critico se** e **Imposta stato del dispositivo su Avviso se**). Nelle proprietà del gruppo di amministrazione è inoltre possibile selezionare altri criteri per definire lo stato del dispositivo mobile.

Per configurare la visualizzazione dei dispositivi Android in Kaspersky Security Center:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Informazioni dispositivo**.
5. Nella sezione **Nome dispositivo in Kaspersky Security Center** selezionare il formato del nome del dispositivo in Administration Console:
   - Modello dispositivo [e-mail, ID dispositivo]
   - Modello dispositivo [e-mail (se presente) o ID dispositivo]

   Un *ID dispositivo* è un ID univoco generato da Kaspersky Endpoint Security for Android a partire dai dati ricevuti da un dispositivo. Per i dispositivi mobili che eseguono Android 10 o versione successiva, Kaspersky Endpoint Security for Android utilizza il SSAID (ID Android) o il checksum di altri dati ricevuti dal dispositivo. Per le versioni precedenti di Android, l'app utilizza l'IMEI.
6. Impostare l'opzione lucchetto nella posizione bloccata ( ).
7. Nella sezione **Stato del dispositivo in Kaspersky Security Center** selezionare lo stato del dispositivo appropriato se un componente di Kaspersky Endpoint Security for Android non funziona: (**Critico**), (**Avviso**) o (**OK**).

   Nell'elenco dei dispositivi mobili lo stato del dispositivo verrà modificato in base allo stato selezionato.
8. Impostare l'opzione lucchetto nella posizione bloccata.
9. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Gestione

Questa sezione contiene informazioni su come gestire in remoto le impostazioni dei dispositivi mobili in Administration Console di Kaspersky Security Center.

Configurazione della connessione a una rete Wi-Fi

Questa sezione fornisce istruzioni su come configurare la connessione automatica a una rete Wi-Fi aziendale nei dispositivi MDM iOS e Android.

Connessione dei dispositivi Android a una rete Wi-Fi

Per connettere il dispositivo mobile a una rete Wi-Fi:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Wi-Fi**.
5. Nella sezione **Reti Wi-Fi** fare clic su **Aggiungi**.

   Verrà visualizzata la finestra **Rete Wi-Fi**.
6. Nel campo **Identificatore del set di servizi (SSID)** immettere il nome della rete Wi-Fi che include il punto di accesso (SSID).
7. Nella sezione **Protezione della rete** selezionare il tipo di sicurezza della rete Wi-Fi (rete aperta o protetta con il protocollo WEP o WPA/WPA2 PSK).
8. Nel campo **Password** impostare una password di accesso alla rete, se è stata selezionata una rete sicura nel passaggio precedente.
9. Nel campo **Porta e indirizzo server proxy** immettere l'indirizzo IP o il nome DNS del server proxy e il numero di porta, se necessario.

   Nei dispositivi che eseguono Android 8.0 o versioni successive le impostazioni del server proxy per il Wi-Fi non possono essere ridefinite con il criterio. Tuttavia, è possibile configurare manualmente le impostazioni del server proxy per una rete Wi-Fi nel dispositivo mobile.

   Se si utilizza un server proxy per la connessione a una rete Wi-Fi, è possibile utilizzare un criterio per configurare le impostazioni per la connessione alla rete. Nei dispositivi che eseguono Android 8.0 o versioni successive è necessario configurare manualmente le impostazioni del server proxy. Nei dispositivi che eseguono Android 8.0 o versioni successive non è possibile utilizzare un criterio per modificare le impostazioni della connessione di rete Wi-Fi, tranne per la password di accesso alla rete.

   Se non si utilizza un server proxy per eseguire la connessione a una rete Wi-Fi, non sono previsti limiti rispetto all'utilizzo dei criteri per gestire una connessione di rete Wi-Fi.
10. Nel campo **Non utilizzare il server proxy per gli indirizzi** generare un elenco di indirizzi Web a cui è possibile accedere senza l'utilizzo del server proxy.

    Ad esempio, è possibile immettere l'indirizzo `example.com`. In questo caso, il server proxy non sarà utilizzato per gli indirizzi `pictures.example.com`, `example.com/movies` e così via. Il protocollo (ad esempio `http://`) può essere omesso.

Nei dispositivi che eseguono Android 8.0 o versioni successive l'esclusione del server proxy per gli indirizzi Web non funziona.

11. Fare clic su **OK**.

    La rete Wi-Fi aggiunta viene visualizzata nell'elenco delle **reti Wi-Fi**.

    È possibile modificare o eliminare le reti Wi-Fi nell'elenco delle reti utilizzando i pulsanti **Modifica** ed **Elimina** nella parte superiore dell'elenco.

12. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. Una volta applicato il criterio nel dispositivo mobile, l'utente può eseguire la connessione alla rete Wi-Fi che è stata aggiunta, senza specificare le impostazioni di rete.

Nei dispositivi che eseguono Android versione 10.0 o successiva se un utente rifiuta di connettersi alla rete Wi-Fi suggerita, l'autorizzazione dell'app per modificare lo stato del Wi-Fi viene revocata. L'utente deve concedere questa autorizzazione manualmente.

Connessione dei dispositivi MDM iOS a una rete Wi-Fi

Per consentire la connessione automatica di un dispositivo MDM iOS a una rete Wi-Fi disponibile e proteggere i dati durante la connessione, è necessario configurare le impostazioni di connessione.

Per configurare la connessione di un dispositivo MDM iOS a una rete Wi-Fi:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Wi-Fi**.
5. Fare clic sul pulsante **Aggiungi** nella sezione **Reti Wi-Fi**.

   Verrà visualizzata la finestra **Rete Wi-Fi**.
6. Nel campo **Identificatore del set di servizi (SSID)** immettere il nome della rete Wi-Fi che include il punto di accesso (SSID).
7. Se si desidera consentire al dispositivo MDM iOS di connettersi automaticamente alla rete Wi-Fi, selezionare la casella **Connessione automatica**.
8. Per impedire la connessione dei dispositivi MDM iOS a una rete Wi-Fi che richiede l'autenticazione preliminare (rete captive), selezionare la casella **Disabilita rilevamento reti captive**.

   Per utilizzare una rete captive, è necessario abbonarsi, accettare un contratto o effettuare un pagamento. Le reti captive possono ad esempio essere distribuite in bar e alberghi.

9. Se si desidera nascondere una rete Wi-Fi nell'elenco delle reti disponibili nel dispositivo MDM iOS, selezionare la casella **Rete nascosta**.

   In questo caso, per connettersi alla rete, l'utente deve immettere manualmente l'Identificatore del set di servizi (SSID) specificato nelle impostazioni del router Wi-Fi nel dispositivo mobile.

10. Nell'elenco a discesa **Protezione della rete** selezionare il tipo di protezione per la connessione alla rete Wi-Fi:

    - **Disabilitata** L'autenticazione dell'utente non è richiesta.
    - **WEP**. La rete è protetta tramite il protocollo WEP (Wireless Encryption Protocol).
    - **WPA/WPA2 (Personal)**. La rete è protetta tramite il protocollo WPA/WPA2 (Wi-Fi Protected Access).
    - **WPA2 (Personal)**. La rete è protetta tramite il protocollo WPA2 (Wi-Fi Protected Access 2.0). La protezione WPA2 è disponibile nei dispositivi che eseguono iOS versione 8 o successiva. WPA2 non è disponibile nei dispositivi Apple TV.
    - **Qualsiasi (Personal)**. La rete è protetta tramite il protocollo di criptaggio WEP, WPA o WPA2, a seconda del tipo di router Wi-Fi. Per l'autenticazione viene utilizzata una chiave di criptaggio univoca per ogni utente.
    - **WEP (Dinamico)**. La rete è protetta tramite il protocollo WEP con l'utilizzo di una chiave dinamica.
    - **WPA/WPA2 (Enterprise)**. La rete è protetta tramite il protocollo di criptaggio WPA/WPA2 con l'utilizzo del protocollo 802.1X.
    - **WPA2 (Enterprise)**. La rete è protetta tramite il protocollo di criptaggio WPA2 con l'utilizzo di una chiave condivisa da tutti gli utenti (802.1X). La protezione WPA2 è disponibile nei dispositivi che eseguono iOS versione 8 o successiva. WPA2 non è disponibile nei dispositivi Apple TV.
    - **Qualsiasi (Enterprise)**. La rete è protetta tramite il protocollo WEP o WPA/WPA2, a seconda del tipo di router Wi-Fi. Per l'autenticazione viene utilizzata una chiave di criptaggio condivisa da tutti gli utenti.

    Se nell'elenco **Protezione della rete** è stato selezionato il valore **WEP (Dinamico)**, **WPA/WPA2 (Enterprise)**, **WPA2 (Enterprise)** o **Qualsiasi (Enterprise)** nella sezione **Protocolli** è possibile selezionare i tipi di protocolli EAP (Extensible Authentication Protocol) per l'identificazione dell'utente nella rete Wi-Fi.

    Nella sezione **Certificati attendibili** è inoltre possibile creare un elenco di certificati attendibili per l'autenticazione dell'utente del dispositivo MDM iOS nei server attendibili.

11. Configurare le impostazioni dell'account per l'autenticazione dell'utente al momento della connessione del dispositivo MDM iOS alla rete Wi-Fi:

    a. Nella sezione **Autenticazione** fare clic sul pulsante **Configura**.

       Verrà visualizzata la finestra **Autenticazione**.

    b. Nel campo **Nome utente** immettere il nome dell'account per l'autenticazione dell'utente al momento della connessione alla rete Wi-Fi.

    c. Per richiedere all'utente di immettere manualmente la password a ogni connessione alla rete Wi-Fi, selezionare la casella **Richiedi password a ogni connessione**.

    d. Nel campo **Password** immettere la password dell'account per l'autenticazione nella rete Wi-Fi.

    e. Nell'elenco a discesa **Certificato di autenticazione** selezionare un certificato per l'autenticazione dell'utente nella rete Wi-Fi. Se l'elenco non contiene certificati, **è possibile aggiungerli nella sezione** Certificati.

f. Nel campo **ID utente** immettere l'ID utente visualizzato durante la trasmissione dei dati al momento dell'autenticazione invece del nome reale dell'utente.

L'ID utente è progettato per rendere più sicuro il processo di autenticazione, dal momento che il nome dell'utente non è visualizzato direttamente, ma viene trasmesso tramite un tunnel TLS criptato.

g. Fare clic su **OK**.

Come risultato, le impostazioni dell'account per l'autenticazione dell'utente al momento della connessione alla rete Wi-Fi saranno configurate nel dispositivo MDM iOS.

12. Se necessario, configurare le impostazioni della connessione alla rete Wi-Fi tramite un server proxy:

a. Nella sezione **Server proxy** fare clic sul pulsante **Configura**.

b. Nella finestra **Server proxy** visualizzata selezionare la modalità di configurazione del server proxy e specificare le impostazioni di connessione.

c. Fare clic su **OK**.

Come risultato, le impostazioni di connessione del dispositivo alla rete Wi-Fi tramite un server proxy vengono configurate nel dispositivo MDM iOS.

13. Fare clic su **OK**.

La nuova rete Wi-Fi viene visualizzata nell'elenco.

14. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, una connessione a una rete Wi-Fi sarà configurata nel dispositivo MDM iOS dell'utente. Il dispositivo mobile dell'utente si connetterà automaticamente alle reti Wi-Fi disponibili. La protezione dei dati durante la connessione a una rete Wi-Fi è assicurata dalla tecnologia di autenticazione.

Configurazione dell'e-mail

Questa sezione contiene informazioni sulla configurazione delle cassette postali nei dispositivi mobili.

Configurazione di una cassetta postale nei dispositivi MDM iOS

Per consentire all'utente di un dispositivo MDM iOS di utilizzare l'e-mail, aggiungere l'account e-mail dell'utente all'elenco degli account nel dispositivo MDM iOS.

Per impostazione predefinita, l'indirizzo e-mail viene aggiunto con le impostazioni seguenti:

- Protocollo e-mail – IMAP.
- L'utente può spostare i messaggi e-mail tra i propri account e sincronizzare gli indirizzi degli account.
- L'utente può utilizzare qualsiasi client e-mail (diverso da Mail) per l'utilizzo della posta elettronica.
- La connessione SSL non viene utilizzata durante la trasmissione dei messaggi.

È possibile modificare le impostazioni specificate durante l'aggiunta dell'account.

Per aggiungere un account e-mail dell'utente del dispositivo MDM iOS:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare **E-mail**.
5. Fare clic sul pulsante **Aggiungi** nella sezione **Account e-mail**.

   Verrà visualizzata la finestra **Account e-mail**.
6. Nel campo **Descrizione** immettere una descrizione dell'account e-mail dell'utente.
7. Selezionare il protocollo e-mail:
   - **POP**
   - **IMAP**
8. Se necessario, specificare il prefisso del percorso IMAP nel campo **Prefisso percorso IMAP**.

   Il prefisso del percorso IMAP deve essere immesso in lettere maiuscole (ad esempio, GMAIL per Google Mail). Questo campo è disponibile se è selezionato il protocollo per gli account IMAP.
9. Nel campo **Nome utente visualizzato nei messaggi** immettere il nome utente da visualizzare nel campo **Da:** per tutti i messaggi in uscita.
10. Nel campo **Indirizzo e-mail** specificare l'indirizzo e-mail dell'utente del dispositivo MDM iOS.
11. Configurare le impostazioni avanzate dell'account e-mail:
    - Per consentire all'utente di spostare i messaggi e-mail tra i propri account, selezionare la casella **Consenti lo spostamento dei messaggi tra gli account**.
    - Per consentire la sincronizzazione degli indirizzi e-mail utilizzati tra gli account utente, selezionare la casella **Consenti sincronizzazione degli indirizzi recenti**.
    - Per consentire a un utente di utilizzare il servizio Mail Drop per inoltrare allegati di grandi dimensioni, selezionare la casella **Consenti Mail Drop**.
    - Per consentire all'utente di utilizzare solo il client e-mail standard di iOS, selezionare la casella **Consenti solo l'utilizzo dell'app Mail**.
12. Configurare le impostazioni per l'utilizzo del protocollo S/MIME nell'app di posta. *S/MIME* è un protocollo per la trasmissione dei messaggi criptati con firma digitale.
    - Per utilizzare il protocollo S/MIME per firmare la posta in uscita, selezionare la casella di controllo **Firma i messaggi** e selezionare un certificato per la firma. Una firma digitale conferma l'autenticità del mittente e indica che i contenuti del messaggio non sono stati modificati durante la trasmissione al destinatario. La firma del messaggio è disponibile nei dispositivi che eseguono iOS versione 10.3 o successiva.
    - Per utilizzare il protocollo S/MIME per criptare la posta in uscita, selezionare la casella di controllo **Cripta i messaggi per impostazione predefinita** e selezionare un certificato per il criptaggio (chiave pubblica). Il criptaggio dei messaggi è disponibile nei dispositivi che eseguono iOS versione 10.3 o successiva.

- Per consentire all'utente di criptare i singoli messaggi, selezionare la casella di controllo **Mostra l'interruttore per criptare i messaggi**. Per inviare messaggi criptati, l'utente deve fare clic sull'icona nell'app di posta nel campo **A**.

13. Nelle sezioni **Server della posta in entrata** e **Server della posta in uscita** fare clic sul pulsante **Impostazioni** per configurare le impostazioni di connessione ai server:

    - **Porta e indirizzo server**: nomi di host o indirizzi IP dei server della posta in entrata e in uscita e numeri di porta dei server.
    - **Nome account**: nome dell'account dell'utente per l'autorizzazione dei server della posta in entrata e in uscita.
    - **Tipo di autenticazione**: tipo di autenticazione dell'account e-mail dell'utente nei server della posta in entrata e in uscita.
    - **Password**: password dell'account per l'autenticazione nei server della posta in entrata e in uscita protetti tramite il metodo di autenticazione selezionato.
    - **Usa una sola password per i server di posta in entrata e in uscita**: utilizzare un'unica password per l'autenticazione degli utenti nei server di posta in entrata e in uscita.
    - **Usa connessione SSL**: utilizzo del protocollo di trasporto dati SSL (Secure Sockets Layer), che utilizza il criptaggio e l'autenticazione basata sul certificato per proteggere la trasmissione dei dati.

14. Fare clic su **OK**.

    Il nuovo account e-mail viene visualizzato nell'elenco.

15. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, gli account e-mail inseriti nell'elenco compilato verranno aggiunti nel dispositivo mobile dell'utente.

Configurazione di una cassetta postale Exchange nei dispositivi MDM iOS

Per consentire all'utente del dispositivo MDM iOS di utilizzare la posta elettronica, il calendario, i contatti, le note e le attività aziendali, aggiungere l'account Exchange ActiveSync dell'utente nel server Microsoft Exchange.

Per impostazione predefinita, un account con le seguenti impostazione viene aggiunto al server Microsoft Exchange:

- La posta elettronica viene sincronizzata una volta alla settimana.
- L'utente può spostare i messaggi tra i propri account e sincronizzare gli indirizzi degli account.
- L'utente può utilizzare qualsiasi client e-mail (diverso da Mail) per l'utilizzo della posta elettronica.
- La connessione SSL non viene utilizzata durante la trasmissione dei messaggi.

È possibile modificare le impostazioni specificate durante l'aggiunta dell'account Exchange ActiveSync.

Per aggiungere un account Exchange ActiveSync dell'utente del dispositivo MDM iOS:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Exchange ActiveSync**.

5. Fare clic sul pulsante **Aggiungi** nella sezione **Account Exchange ActiveSync**.

   Verrà visualizzata la finestra **Account Exchange ActiveSync** nella scheda **Generale**.

6. Nel campo **Nome account** immettere il nome dell'account per l'autorizzazione nel server Microsoft Exchange. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

7. Nel campo **Indirizzo server** immettere il nome di rete o l'indirizzo IP del server Microsoft Exchange.

8. Per utilizzare il protocollo di trasporto dati SSL (Secure Sockets Layer) per proteggere la trasmissione dei dati, selezionare la casella **Usa connessione SSL**.

9. Nel campo **Dominio** immettere il nome del dominio dell'utente del dispositivo MDM iOS. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

10. Nel campo **Nome account utente** immettere il nome dell'utente del dispositivo MDM iOS.

    Se si lascia vuoto questo campo, Kaspersky Device Management for iOS richiede all'utente di immettere il nome utente al momento dell'applicazione del criterio nel dispositivo MDM iOS. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

11. Nel campo **Indirizzo e-mail** specificare l'indirizzo e-mail dell'utente del dispositivo MDM iOS. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

12. Nel campo **Password** immettere la password dell'account Exchange ActiveSync per l'autorizzazione nel server Microsoft Exchange.

13. Selezionare la scheda **Avanzate** e quindi configurare le impostazioni avanzate dell'account Exchange ActiveSync:

    - **Numero di giorni per la sincronizzazione della posta per <periodo di tempo>**
    - **Tipo di autenticazione**
    - **Consenti lo spostamento dei messaggi tra gli account**
    - **Consenti sincronizzazione degli indirizzi recenti**
    - **Consenti solo l'utilizzo dell'app Mail**

14. Configurare le impostazioni per l'utilizzo del protocollo S/MIME nell'app di posta. *S/MIME* è un protocollo per la trasmissione dei messaggi criptati con firma digitale.

    - Per utilizzare il protocollo S/MIME per firmare la posta in uscita, selezionare la casella di controllo **Firma i messaggi** e selezionare un certificato per la firma. Una firma digitale conferma l'autenticità del mittente e indica che i contenuti del messaggio non sono stati modificati durante la trasmissione al destinatario. La firma del messaggio è disponibile nei dispositivi che eseguono iOS versione 10.3 o successiva.

    - Per utilizzare il protocollo S/MIME per criptare la posta in uscita, selezionare la casella di controllo **Cripta i messaggi per impostazione predefinita** e selezionare un certificato per il criptaggio (chiave pubblica). Il criptaggio dei messaggi è disponibile nei dispositivi che eseguono iOS versione 10.3 o successiva.

- Per consentire all'utente di criptare i singoli messaggi, selezionare la casella di controllo **Mostra l'interruttore per criptare i messaggi**. Per inviare messaggi criptati, l'utente deve fare clic sull'icona nell'app di posta nel campo **A**.

15. Fare clic su **OK**.

    Il nuovo account Exchange ActiveSync viene visualizzato nell'elenco.

16. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, gli account Exchange ActiveSync inseriti nell'elenco compilato verranno aggiunti nel dispositivo mobile dell'utente.

Configurazione di una cassetta postale Exchange nei dispositivi Android (solo Samsung)

Per utilizzare posta aziendale, contatti e calendario in un dispositivo mobile, è necessario configurare le impostazioni della cassetta postale Exchange.

La configurazione di una cassetta postale di Exchange è possibile solo per i dispositivi Samsung.

Per configurare una cassetta postale Exchange in un dispositivo mobile:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Gestisci Samsung KNOX → Gestisci dispositivo Samsung**.
5. Nella finestra **Exchange ActiveSync** fare clic sul pulsante **Configura**.

   Verrà visualizzata la finestra **Impostazioni server e-mail Exchange**.
6. Nel campo **Indirizzo server** immettere l'indirizzo IP o il nome DNS del server che ospita il server di posta.
7. Nel campo **Dominio** immettere il nome del dominio dell'utente del dispositivo mobile nella rete aziendale.
8. Nell'elenco a discesa **Intervallo di sincronizzazione** selezionare l'intervallo desiderato per la sincronizzazione del dispositivo mobile con il server Microsoft Exchange.
9. Per utilizzare il protocollo di trasporto dati SSL (Secure Sockets Layer), selezionare la casella **Usa connessione SSL**.
10. Per utilizzare certificati digitali per proteggere il trasferimento dei dati tra il dispositivo mobile e il server Microsoft Exchange, selezionare la casella **Verifica certificato server**.
11. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Gestione delle app mobili di terze parti

È possibile utilizzare i contenitori per monitorare l'attività delle applicazioni avviate nel dispositivo mobile dell'utente. *Un contenitore* è uno speciale involucro per le app mobili, che rende possibile il controllo dell'attività dell'app inserita nel contenitore, garantendo la protezione dei dati personali e aziendali dell'utente nel dispositivo.

In Kaspersky Security for Mobile Service Pack 3 Maintenance Release 2 non è più disponibile il supporto per la creazione di contenitori per le app mobili. Tuttavia, i contenitori creati nelle versioni precedenti dell'applicazione possono essere aggiunti ai dispositivi Android.

È possibile installare un'app inserita in un contenitore nel dispositivo dell'utente in uno dei modi seguenti:

- Inviando all'utente un messaggio e-mail con un collegamento al pacchetto di installazione dell'app nel contenitore.
- Specificando un'app inserita in un contenitore come app richiesta o consentita nella sezione **Controllo app** della finestra delle proprietà del criterio. Dopo la sincronizzazione del dispositivo mobile con Kaspersky Security Center, il pacchetto di distribuzione dell'app nel contenitore viene copiato automaticamente nel dispositivo dell'utente.

Per installare app inserite in un contenitore, nel dispositivo mobile dell'utente deve essere consentita l'installazione di app da origini sconosciute. Per proteggere il dispositivo e i dati dell'utente in seguito all'installazione di app inserite in un contenitore, è consigliabile vietare l'installazione di app da origini sconosciute. Per ulteriori informazioni sull'installazione delle app senza Google Play, fare riferimento alla *Guida Android*.

Configurazione delle notifiche per Kaspersky Endpoint Security for Android

Se si desidera che l'utente del dispositivo mobile non venga distratto dalle notifiche di Kaspersky Endpoint Security for Android, è possibile disabilitare determinate notifiche.

Kaspersky Endpoint Security utilizza i seguenti strumenti per visualizzare lo stato della protezione del dispositivo:

- **Notifica relativa allo stato della protezione**. Questa notifica viene visualizzata nella barra delle notifiche. La notifica relativa allo stato della protezione non può essere rimossa. La notifica visualizza lo stato della protezione del dispositivo (ad esempio) e il numero di problemi, se presenti. È possibile toccare lo stato della protezione del dispositivo e visualizzare i problemi elencati nell'app.
- **Notifiche dell'app**. Queste notifiche danno informazioni sull'applicazione all'utente del dispositivo (ad esempio sul rilevamento delle minacce).
- **Messaggi pop-up**. I messaggi pop-up richiedono l'intervento dell'utente del dispositivo (ad esempio quando viene rilevata una minaccia).

Tutte le notifiche di Kaspersky Endpoint Security for Android sono abilitate per impostazione predefinita.

L'utente di un dispositivo Android può disabilitare tutte le notifiche di Kaspersky Endpoint Security for Android nelle impostazioni nella barra di notifica. Se le notifiche sono disabilitate, l'utente non monitora l'esecuzione dell'app e potrebbe ignorare informazioni importanti (ad esempio, le informazioni sugli errori durante la sincronizzazione del dispositivo con Kaspersky Security Center). In questo caso, per visualizzare lo stato dell'app, l'utente deve aprire Kaspersky Endpoint Security for Android.

Per configurare la visualizzazione delle notifiche sull'esecuzione di Kaspersky Endpoint Security for Android:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Avanzate**.
5. Nella sezione **Notifiche dell'app** fare clic sul pulsante **Configura**.

   Verrà visualizzata la finestra **Impostazioni di notifica del dispositivo**.
6. Selezionare i problemi di Kaspersky Endpoint Security for Android che si desidera nascondere nel dispositivo mobile dell'utente e fare clic sul pulsante **OK**.

   Kaspersky Endpoint Security for Android non visualizzerà i problemi nella notifica sullo stato della protezione né la sezione **Stato** nell'app. Kaspersky Endpoint Security for Android continuerà a visualizzare la notifica sullo stato della protezione e le notifiche delle app.

   Alcuni problemi di Kaspersky Endpoint Security for Android sono obbligatori e non possono essere disabilitati (ad esempio i problemi sulla scadenza della licenza).
7. Per nascondere tutte le notifiche e i messaggi pop-up, selezionare **Disabilita notifiche e pop-up quando l'app è in background**.

   Kaspersky Endpoint Security for Android visualizzerà solo la notifica sullo stato della protezione. La notifica visualizza lo stato della protezione del dispositivo (ad esempio) e il numero di problemi. L'app visualizzerà le notifiche anche quando l'utente utilizza l'app (ad esempio aggiorna manualmente i database anti-virus).

   Gli esperti di Kaspersky hanno raccomandato di abilitare notifiche e i messaggi pop-up. Se si disabilitano le notifiche e i messaggi pop-up quando l'app è in background, l'app non avviserà gli utenti delle minacce in tempo reale. Gli utenti dei dispositivi mobili possono scoprire lo stato della protezione del dispositivo solo quando aprono l'app.
8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. Le notifiche di Kaspersky Endpoint Security for Android disabilitate non saranno visualizzate nel dispositivo mobile dell'utente.

Connessione dei dispositivi MDM iOS ad AirPlay

Configurare la connessione ai dispositivi AirPlay per consentire lo streaming di musica, foto e video dal dispositivo MDM iOS ai dispositivi AirPlay. Per utilizzare la tecnologia AirPlay, il dispositivo mobile e i dispositivi AirPlay devono essere connessi alla stessa rete wireless. I dispositivi AirPlay includono dispositivi Apple TV (di seconda e terza generazione), dispositivi AirPort Express e altoparlanti o radio con supporto per AirPlay.

La connessione automatica ai dispositivi AirPlay è disponibile solo per i dispositivi controllati.

Per configurare la connessione di un dispositivo MDM iOS ai dispositivi AirPlay:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **AirPlay**.
5. Nella sezione **Dispositivi AirPlay** selezionare la casella **Applica impostazioni nel dispositivo**.
6. Fare clic sul pulsante **Aggiungi** nella sezione **Password**.

   Nella tabella delle password verrà aggiunta una riga vuota.
7. Nella colonna **Nome dispositivo** immettere il nome del dispositivo AirPlay nella rete wireless.
8. Nella colonna **Password** immettere la password per il dispositivo AirPlay.
9. Per limitare l'accesso dei dispositivi MDM iOS ai dispositivi AirPlay, creare un elenco di dispositivi consentiti nella sezione **Dispositivi consentiti**. A tale scopo, aggiungere gli indirizzi MAC dei dispositivi AirPlay all'elenco dei dispositivi consentiti.

   L'accesso ai dispositivi AirPlay che non sono inseriti nell'elenco dei dispositivi consentiti viene bloccato. Se l'elenco dei dispositivi consentiti viene lasciato vuoto, Kaspersky Device Management for iOS consente l'accesso a tutti i dispositivi AirPlay.
10. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, il dispositivo mobile dell'utente si connetterà automaticamente ai dispositivi AirPlay per lo streaming di contenuti multimediali.

Connessione dei dispositivi MDM iOS ad AirPrint

Per consentire la stampa di documenti dal dispositivo MDM iOS in modalità wireless utilizzando la tecnologia AirPrint, configurare la connessione automatica alle stampanti AirPrint. Il dispositivo mobile e la stampante devono essere connessi alla stessa rete wireless. È necessario configurare l'accesso condiviso per tutti gli utenti nella stampante AirPrint.

Per configurare la connessione di un dispositivo MDM iOS a una stampante AirPrint:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **AirPrint**.
5. Fare clic sul pulsante **Aggiungi** nella sezione **Stampanti AirPrint**.

   Verrà visualizzata la finestra **Stampante**.
6. Nel campo **Indirizzo IP** immettere l'indirizzo IP della stampante AirPrint.
7. Nel campo **Percorso risorsa** immettere il percorso della stampante AirPrint.

Il percorso della stampante corrisponde alla chiave rp (percorso della risorsa) del protocollo Bonjour. Ad esempio:

- stampanti/Canon_MG5300_series
- ipp/stampa
- Stampante_Epson_IPP

8. Fare clic su **OK**.

   La stampante AirPrint aggiunta verrà visualizzata nell'elenco.

9. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, il dispositivo mobile potrà stampare documenti in modalità wireless tramite la stampante AirPrint.

Configurazione del nome punto di accesso (APN)

Per connettere un dispositivo mobile ai servizi di trasferimento dei dati in una rete mobile, è necessario configurare le impostazioni del nome punto di accesso (APN).

Configurazione della APN nei dispositivi Android (solo Samsung)

La configurazione dell'APN è possibile solo per i dispositivi Samsung.

È necessario inserire una scheda SIM per essere in grado di utilizzare un punto di accesso nel dispositivo mobile dell'utente. Le impostazioni del punto di accesso vengono fornite dall'operatore di telefonia mobile. Impostazioni non corrette del punto di accesso possono comportare spese telefoniche aggiuntive.

Per configurare le impostazioni del nome punto di accesso (APN):

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Gestisci Samsung KNOX → APN**.
5. Nella sezione **APN** fare clic sul pulsante **Configura**.

   Verrà visualizzata la finestra **Impostazioni APN**.

6. Nella scheda **Generale** specificare le seguenti impostazioni del punto di accesso:

   a. Nell'elenco a discesa **Tipo APN** selezionare il tipo di punto di accesso.

   b. Nel campo **Nome APN** specificare il nome del punto di accesso.

c. Nel campo **MCC** immettere il codice MCC (Mobile Country Code).

d. Nel campo **MNC** immettere il codice MNC (Mobile Network Code).

e. Se è stato selezionato **MMS** o **Internet e MMS** come tipo di punto di accesso, specificare le seguenti impostazioni aggiuntive per gli MMS:

- Nel campo **Server MMS** specificare il nome di dominio completo del server dell'operatore di telefonia mobile utilizzato per lo scambio di MMS.
- Nel campo **Server proxy MMS** specificare il nome di rete o l'indirizzo IP del server proxy e il numero di porta del server dell'operatore di telefonia mobile utilizzato per lo scambio di MMS.

7. Nella scheda **Avanzate** configurare le impostazioni avanzate del nome punto di accesso (APN):

a. Nell'elenco a discesa **Tipo di autenticazione** selezionare il tipo di autenticazione del dispositivo mobile dell'utente nel server dell'operatore di telefonia mobile per l'accesso alla rete.

b. Nel campo **Indirizzo server** specificare il nome di rete del server dell'operatore di telefonia mobile tramite il quale viene eseguito l'accesso ai servizi di trasmissione dei dati.

c. Nel campo **Indirizzo server proxy** specificare il nome di rete o l'indirizzo IP e il numero di porta del server proxy dell'operatore di telefonia mobile per l'accesso alla rete.

d. Nel campo **Nome utente** immettere il nome utente per l'autorizzazione nella rete mobile.

e. Nel campo **Password** immettere la password per l'autorizzazione dell'utente nella rete mobile.

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione della APN nei dispositivi MDM iOS

Il nome del punto di accesso (APN) deve essere configurato allo scopo di abilitare il servizio di trasmissione dati in una rete mobile nel dispositivo MDM iOS dell'utente.

La sezione **APN** non è aggiornata. È consigliabile configurare le impostazioni APN nella sezione **Comunicazioni cellulari**. Prima di configurare le impostazioni delle comunicazioni cellulari, verificare che le impostazioni della sezione **APN** non siano state applicate nel dispositivo (la casella **Applica impostazioni nel dispositivo** è deselezionata). Le impostazioni delle sezioni **APN** e **Comunicazioni cellulari** non possono essere utilizzate simultaneamente.

Per configurare un punto di accesso nel dispositivo MDM iOS di un utente:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Comunicazioni cellulari**.

5. Nella sezione **Impostazioni delle comunicazioni cellulari** selezionare la casella **Applica impostazioni nel dispositivo**.

6. Nell'elenco dei **Tipo APN** selezionare il tipo di punto di accesso per il trasferimento dei dati in una rete mobile GPRS/3G/4G:

   - **APN predefinito**: configurazione delle impostazioni delle comunicazioni cellulari per il trasferimento dei dati tramite un operatore di rete mobile che supporta il funzionamento con una SIM Apple predefinita. Per maggiori informazioni sui dispositivi con una SIM Apple predefinita, visitare il sito Web dell'assistenza tecnica Apple.

   - **APN**: configurazione delle impostazioni delle comunicazioni cellulari per il trasferimento dei dati tramite l'operatore di rete mobile della scheda SIM inserita.

   - **APN predefinito e APN**: configurazione delle impostazioni delle comunicazioni cellulari per il trasferimento dei dati tramite gli operatori di rete mobile della scheda SIM inserita e della SIM Apple predefinita. Per maggiori informazioni sui dispositivi con una SIM Apple predefinita e con uno slot per la scheda SIM, visitare il sito Web dell'assistenza tecnica Apple.

7. Nel campo **Nome APN** specificare il nome del punto di accesso.

8. Nell'elenco a discesa **Tipo di autenticazione** selezionare il tipo di autenticazione utente per il dispositivo sul server dell'operatore di telefonia mobile per l'accesso alla rete (Internet e MMS):

9. Nel campo **Nome utente** immettere il nome utente per l'autorizzazione nella rete mobile.

10. Nel campo **Password** immettere la password per l'autorizzazione dell'utente nella rete mobile.

11. Nel campo **Porta e indirizzo server proxy** immettere il nome di un host o l'indirizzo IP di un server proxy e il numero della porta del server proxy.

12. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, il nome del punto di accesso (APN) viene configurato nel dispositivo mobile dell'utente.

Configurazione del profilo lavoro Android

Questa sezione contiene informazioni sull'utilizzo di un profilo lavoro Android.

Informazioni sul profilo lavoro Android

Android Enterprise è una piattaforma per la gestione dell'infrastruttura mobile aziendale, che fornisce ai dipendenti aziendali un ambiente di lavoro in cui possono utilizzare i dispositivi mobili. Per informazioni dettagliate sull'utilizzo di Android Enterprise, consultare il sito Web dell'assistenza di Google.

È possibile creare il profilo lavoro Android (di seguito denominato anche "profilo lavoro") nel dispositivo mobile dell'utente. Il *profilo lavoro Android* è un ambiente sicuro nel dispositivo dell'utente in cui l'amministratore può gestire app e account utente senza limitare l'utilizzo dei dati personali da parte dell'utente. Quando nel dispositivo mobile dell'utente viene creato un profilo lavoro, in quest'ultimo vengono automaticamente installate le seguenti app aziendali: Google Play Market, Google Chrome, Download, Kaspersky Endpoint Security for Android e così via. Le app aziendali installate nel profilo lavoro e le notifiche di tali app sono contrassegnate con l'icona . È necessario creare un account aziendale Google separato per l'account Google Play Market. Le app installate nel profilo lavoro vengono visualizzate nell'elenco standard delle app.

Configurazione del profilo lavoro

Per configurare le impostazioni del profilo lavoro Android:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare il **profilo lavoro Android**.
5. Nell'area di lavoro **Profilo lavoro Android** selezionare la casella di controllo **Crea profilo lavoro**.
6. Specificare le impostazioni del profilo lavoro:

   - Per abilitare Controllo app nel profilo lavoro Android e disabilitarlo nel profilo personale, selezionare la casella **Abilita Controllo app solo nel profilo lavoro**.

     Nella sezione **Utenti** è possibile selezionare **Controllo app** e utilizzare l'area di lavoro per creare elenchi di app richieste, consigliate, bloccate e consentite, nonché categorie di app bloccate e consentite nella sezione.

   - Per abilitare Protezione Web per Google Chrome nel profilo lavoro e disabilitarlo nel profilo personale, nell'area di lavoro della sezione **Profilo lavoro Android** selezionare la casella di controllo **Abilita Protezione Web solo nel profilo lavoro**.

     Protezione Web per Samsung Internet Browser blocca i siti nei profili lavoro e personali. Non è possibile abilitare Protezione Web per Samsung Internet Browser solo nel profilo lavoro. Per utilizzare Protezione Web per Samsung Internet Browser nel profilo lavoro, disabilitare l'opzione **Abilita Protezione Web solo nel profilo lavoro**. Se questa opzione è abilitata, Protezione Web per Samsung Internet Browser non viene eseguito. Protezione Web nel profilo lavoro è disabilitato per impostazione predefinita.

     > Protezione Web nei dispositivi Android funziona solo nel browser Google Chrome e in Samsung Internet Browser.

     È possibile specificare le impostazioni di accesso ai siti Web (creando un elenco di categorie di siti Web bloccati o un elenco di siti Web consentiti) nella sezione **Protezione Web**.

   - Per impedire all'utente di copiare dati tramite gli Appunti dalle app nel profilo lavoro alle app personali, selezionare la casella **Impedisci il trasferimento di dati dal profilo lavoro a quello personale**.

   - Per impedire all'utente di utilizzare la modalità debug USB sul dispositivo mobile nel profilo di lavoro, selezionare la casella **Impedisci l'attivazione della modalità debug USB**.

     Nella modalità debug USB l'utente può ad esempio scaricare un'app utilizzando una workstation.

- Per impedire all'utente di installare app nel profilo lavoro Android da tutte le origini tranne Google Play, selezionare la casella **Impedisci l'installazione di app nel profilo lavoro da origini sconosciute**.

- Per impedire all'utente di rimuovere app dal profilo lavoro Android, selezionare la casella **Impedisci la rimozione di app dal profilo lavoro**.

7. Per configurare le impostazioni del profilo lavoro nel dispositivo mobile dell'utente, bloccare le modifiche alle impostazioni.

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. Lo spazio del dispositivo mobile dell'utente è suddiviso in un profilo lavoro e un profilo personale.

Aggiunta di un account LDAP

Per consentire all'utente del dispositivo MDM iOS di accedere ai contatti aziendali nel server LDAP, aggiungere l'account LDAP.

Per aggiungere l'account LDAP dell'utente del dispositivo MDM iOS:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **LDAP**.

5. Fare clic sul pulsante **Aggiungi** nella sezione **Account LDAP**.

   Verrà visualizzata la finestra **Account LDAP**.

6. Nel campo **Descrizione** immettere una descrizione dell'account LDAP dell'utente. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

7. Nel campo **Nome account** immettere il nome dell'account per l'autorizzazione nel server LDAP. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

8. Nel campo **Password** immettere la password dell'account LDAP per l'autorizzazione nel server LDAP.

9. Nel campo **Indirizzo server** immettere il nome del dominio del server LDAP. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

10. Per utilizzare il protocollo di trasporto dati SSL (Secure Sockets Layer) per proteggere la trasmissione dei messaggi, selezionare la casella **Usa connessione SSL**.

11. Compilare un elenco di query di ricerca per l'accesso dell'utente del dispositivo mobile MDM iOS ai dati aziendali nel server LDAP:

    a. Fare clic sul pulsante **Aggiungi** nella sezione **Impostazioni di ricerca**.

       Nella tabella con le query di ricerca verrà visualizzata una riga vuota.

b. Nella colonna **Nome** immettere il nome di una query di ricerca.

c. Nella colonna **Ambito di ricerca** selezionare il livello di nidificazione della cartella per la ricerca dei dati aziendali nel server LDAP:

- **Base** – ricerca nella cartella di base del server LDAP.
- **Un livello** – ricerca nelle cartelle al primo livello di nidificazione a partire dalla cartella di base.
- **Sottostruttura** – ricerca nelle cartelle a tutti i livelli di nidificazione a partire dalla cartella di base.

d. Nella colonna **Base di ricerca** immettere il percorso della cartella nel server LDAP in cui ha inizio la ricerca (ad esempio: "ou=people", "o=esempio corp").

e. Ripetere i passaggi a-d per tutte le query di ricerca che si desidera aggiungere al dispositivo MDM iOS.

12. Fare clic su **OK**.

    Il nuovo account LDAP viene visualizzato nell'elenco.

13. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, gli account LDAP inseriti nell'elenco compilato verranno aggiunti nel dispositivo mobile dell'utente. L'utente può accedere ai contatti aziendali nelle app iOS standard: Contatti, Messaggi e Mail.

Aggiunta di un account per il calendario

Per consentire all'utente del dispositivo MDM iOS di accedere agli eventi del proprio calendario nel server CalDAV, aggiungere l'account CalDAV. La sincronizzazione con il server CalDAV consente all'utente di creare e ricevere inviti, ricevere aggiornamenti degli eventi e sincronizzare le attività con l'app Promemoria.

Per aggiungere l'account CalDAV dell'utente del dispositivo MDM iOS:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Calendario**.
5. Fare clic sul pulsante **Aggiungi** nella sezione **Account CalDAV**.

   Verrà visualizzata la finestra **Account CalDAV**.
6. Nel campo **Descrizione** immettere una descrizione dell'account CalDAV dell'utente.
7. Nel campo **Porta e indirizzo server** immettere il nome di un host o l'indirizzo IP di un server CalDAV e il numero della porta del server CalDAV.
8. Nel campo **URL principale** specificare l'URL dell'account CalDAV dell'utente del dispositivo MDM iOS nel server CalDAV (ad esempio: http://esempio.com/caldav/utenti/azienda/utente).

   L'URL deve iniziare con `"http://"` o `"https://"`.

9. Nel campo **Nome account** immettere il nome dell'account per l'autorizzazione nel server CalDAV.

10. Nel campo **Password** impostare la password dell'account CalDAV per l'autorizzazione nel server CalDAV.

11. Per utilizzare il protocollo di trasporto dati SSL (Secure Sockets Layer) per proteggere la trasmissione dei dati sugli eventi tra il server CalDAV e il dispositivo mobile, selezionare la casella **Usa connessione SSL**.

12. Fare clic su **OK**.

    Il nuovo account CalDAV viene visualizzato nell'elenco.

13. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, gli account CalDAV inseriti nell'elenco compilato verranno aggiunti nel dispositivo mobile dell'utente.

Aggiunta di un account per i contatti

Per consentire all'utente del dispositivo MDM iOS di sincronizzare i dati con il server CardDAV, aggiungere l'account CardDAV. La sincronizzazione con il server CardDAV consente all'utente di accedere ai dettagli sui contatti da qualsiasi dispositivo.

Per aggiungere l'account CardDAV dell'utente del dispositivo MDM iOS:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Contatti**.

5. Fare clic sul pulsante **Aggiungi** nella sezione **Account CardDAV**.

   Verrà visualizzata la finestra **Account CardDAV**.

6. Nel campo **Descrizione** immettere una descrizione dell'account CardDAV dell'utente. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

7. Nel campo **Porta e indirizzo server** immettere il nome di un host o l'indirizzo IP di un server CardDAV e il numero della porta del server CardDAV.

8. Nel campo **URL principale** specificare l'URL dell'account CardDAV dell'utente del dispositivo MDM iOS nel server CardDAV (ad esempio: http://esempio.com/carddav/utenti/azienda/utente).

   L'URL deve iniziare con `"http://"` o `"https://"`.

9. Nel campo **Nome account** immettere il nome dell'account per l'autorizzazione nel server CardDAV. È possibile utilizzare le macro disponibili nell'elenco a discesa **Macro disponibili**.

10. Nel campo **Password** impostare la password dell'account CardDAV per l'autorizzazione nel server CardDAV.

11. Per utilizzare il protocollo di trasporto dati SSL (Secure Sockets Layer) per proteggere la trasmissione dei contatti tra il server CardDAV e il dispositivo mobile, selezionare la casella **Usa connessione SSL**.

12. Fare clic su **OK**.

Il nuovo account CardDAV viene visualizzato nell'elenco.

13. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, gli account CardDAV inseriti nell'elenco compilato verranno aggiunti nel dispositivo mobile dell'utente.

Configurazione della sottoscrizione a un calendario

Per consentire all'utente del dispositivo MDM iOS di aggiungere gli eventi di calendari condivisi (ad esempio, il calendario aziendale) al proprio calendario, aggiungere una sottoscrizione al calendario. I *calendari condivisi* sono calendari di altri utenti con un account CalDAV, calendari iCal e altri calendari pubblici.

Per aggiungere un abbonamento al calendario:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Abbonamento al calendario**.
5. Fare clic sul pulsante **Aggiungi** nella sezione **Abbonamenti al calendario**.

   Verrà visualizzata la finestra **Abbonamento al calendario**.
6. Nel campo **Descrizione** immettere una descrizione dell'abbonamento al calendario.
7. Nel campo **Indirizzo Web server** specificare l'URL del calendario di terze parti.

   In questo campo è possibile immettere l'URL dell'account CalDAV dell'utente a cui appartiene il calendario a cui si esegue la sottoscrizione. È anche possibile specificare l'URL di un calendario iCal o di un altro calendario pubblico.
8. Nel campo **Nome utente** immettere il nome dell'account utente per l'autenticazione nel server del calendario di terze parti.
9. Nel campo **Password** immettere la password dell'abbonamento al calendario per l'autenticazione nel server del calendario di terze parti.
10. Per utilizzare il protocollo di trasporto dati SSL (Secure Sockets Layer) per proteggere la trasmissione dei dati sugli eventi tra il server CalDAV e il dispositivo mobile, selezionare la casella **Usa connessione SSL**.
11. Fare clic su **OK**.
12. Il nuovo abbonamento al calendario viene visualizzata nell'elenco.
13. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, gli eventi del calendario condiviso inserito nell'elenco verranno aggiunti nel calendario nel dispositivo mobile dell'utente.

Aggiunta di clip Web

Un *clip Web* è un'app che apre un sito Web dalla schermata iniziale del dispositivo mobile. Facendo clic sulle icone dei clip Web nella schermata iniziale del dispositivo, l'utente può aprire rapidamente i siti Web (come ad esempio il sito Web aziendale). È possibile aggiungere clip Web ai dispositivi degli utenti e configurare l'aspetto dell'icona del clip Web visualizzata sullo schermo.

Per impostazione predefinita, vengono applicate le seguenti restrizioni per l'utilizzo dei clip Web:

- L'utente non può rimuovere manualmente i clip Web dal dispositivo mobile.
- I siti Web aperti quando l'utente fa clic sull'icona di un clip Web non vengono visualizzati in modalità a schermo intero.
- Gli effetti visivi per l'arrotondamento degli angoli, l'ombreggiatura e la finitura lucida vengono applicati alle icone dei clip Web sullo schermo.

Per aggiungere un clip Web nel dispositivo MDM iOS di un utente:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Clip Web**.
5. Fare clic sul pulsante **Aggiungi** nella sezione **Clip Web**.

   Verrà visualizzata la finestra **Clip Web**.
6. Nel campo **Nome** immettere il nome del clip Web da visualizzare nella schermata iniziale del dispositivo MDM iOS.
7. Nel campo **URL** immettere l'indirizzo Web del sito Web aperto facendo clic sull'icona del clip Web. L'indirizzo deve iniziare con `"http://"` o `"https://"`.
8. Per consentire all'utente di rimuovere un clip Web dal dispositivo MDM iOS, selezionare la casella **Consenti rimozione**.
9. Fare clic sul pulsante **Seleziona**, quindi specificare il file con l'immagine per l'icona del clip Web.

   L'icona viene visualizzata nella schermata iniziale del dispositivo MDM iOS. L'immagine deve soddisfare i seguenti requisiti:

   - Dimensioni dell'immagine non superiori a 400 x 400 pixel
   - Formato del file: GIF, JPEG, o PNG
   - Dimensione del file non superiore a 1 MB

   L'icona del clip Web può essere visualizzata in anteprima nel campo **Icona**. Se non si seleziona un'immagine per il clip Web, come icona viene visualizzato un quadrato vuoto.

   Se si desidera che l'icona del clip Web venga visualizzata senza speciali effetti visivi (arrotondamento degli angoli dell'icona e finitura lucida), selezionare la casella **Icona precomposta**.
10. Se si desidera che il sito Web venga aperto in modalità a schermo intero nel dispositivo MDM iOS quando si fa clic sull'icona, selezionare la casella **Clip Web a schermo intero**.

11. Fare clic su **OK**.

    Il nuovo clip Web viene visualizzato nell'elenco.

12. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, le icone dei clip Web inserite nell'elenco creato verranno aggiunte nella schermata iniziale del dispositivo mobile dell'utente.

Aggiunta di caratteri

Per aggiungere un carattere nel dispositivo MDM iOS di un utente:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi iOS MDM.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic.
4. Nella finestra **Proprietà** selezionare la sezione **Caratteri**.
5. Fare clic sul pulsante **Aggiungi** nella sezione **Caratteri**.

   Verrà visualizzata la finestra **Carattere**.

6. Nel campo **Nome file** specificare il percorso del file di un tipo di carattere (un file con estensione .ttf o .otf).

   I caratteri con estensione ttc o otc non sono supportati.

   I caratteri sono identificati tramite il nome PostScript. Non installare caratteri con lo stesso nome PostScript, anche se il contenuto è differente. L'installazione di caratteri con lo stesso nome PostScript genererà un errore non definito.

7. Fare clic su **Apri**.

   Il nuovo carattere viene visualizzato nell'elenco.

8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Come risultato, una volta applicato il criterio, all'utente verrà richiesto di installare i caratteri inseriti nell'elenco creato.

Gestione dell'app utilizzando sistemi EMM di terze parti (solo Android)

È possibile utilizzare l'app Kaspersky Endpoint Security for Android senza i sistemi di amministrazione di Kaspersky. Utilizzare le soluzioni di altri provider di servizi EMM (Enterprise Mobility Management) per distribuire e gestire l'app Kaspersky Endpoint Security for Android. Kaspersky partecipa alla community AppConfig per garantire il funzionamento dell'app con soluzioni EMM di terze parti.

È possibile gestire l'app Kaspersky Endpoint Security for Android tramite soluzioni EMM di terze parti solo nei dispositivi Android.

È possibile utilizzare le soluzioni EMM di terze parti solo per distribuire l'app Kaspersky Endpoint Security for Android. Connettere il dispositivo a Kaspersky Security Center e gestire l'app in Administration Console. In questo caso, la gestione dell'app Kaspersky Endpoint Security for Android nella console EMM non sarà disponibile.

Se è stata distribuita l'app Kaspersky Endpoint Security for Android utilizzando il sistema EMM di terze parti, è impossibile gestire l'app in Kaspersky Endpoint Security Cloud. È possibile gestire l'app Kaspersky Endpoint Security for Android nella console EMM.

Le seguenti soluzioni EMM supportano l'utilizzo dell'app Kaspersky Endpoint Security for Android:

- VMware AirWatch
- MobileIron
- IBM Maas360
- Microsoft Intune
- SOTI MobiControl

È possibile eseguire le seguenti operazioni nella console EMM:

- Distribuire l'app a un profilo lavoro Android nei dispositivi degli utenti.
- Attivare l'app.
- Configurare le impostazioni dell'app:
  - Abilitare la protezione contro i siti Web dannosi e di phishing su Internet.
  - Configurare le impostazioni per la connessione del dispositivo a Kaspersky Security Center.
  - Configurare le impostazioni di Anti-Virus.
  - Configurare la pianificazione per l'esecuzione di una scansione virus nel dispositivo.
  - Abilitare il rilevamento di adware e app che possono essere utilizzate da utenti malintenzionati per danneggiare il dispositivo o i dati personali dell'utente.
  - Configurare la pianificazione per gli aggiornamenti dei database dell'app.

Introduzione

Per distribuire l'app nei dispositivi mobili degli utenti, è necessario aggiungere Kaspersky Endpoint Security for Android all'archivio di app EMM. È possibile aggiungere Kaspersky Endpoint Security for Android all'archivio di app EMM utilizzando il collegamento di Google Play. Per maggiori informazioni sull'utilizzo delle app nella console EMM, visitare il *sito Web dell'assistenza tecnica del fornitore del servizio EMM*.

L'app Kaspersky Endpoint Security for Android è distribuita in un profilo lavoro Android. L'app è isolata dai dati personali dell'utente e protegge solo i dati aziendali nel profilo di lavoro. È consigliabile verificare che Kaspersky Endpoint Security for Android sia protetto dalla rimozione tramite gli strumenti della console EMM.

Come installare l'app

A seconda della console EMM, selezionare il metodo per l'installazione dell'app nei dispositivi: installazione invisibile all'utente, invio di un'e-mail contenente un collegamento all'app in Google Play o un altro metodo disponibile.

Le seguenti autorizzazioni sono necessarie per il funzionamento dell'app:

- Autorizzazione relativa alla memoria per l'accesso ai file quando è in esecuzione Anti-Virus (solo per Android 6.0 o versioni successive).
- Autorizzazione relativa al telefono per l'identificazione del dispositivo, ad esempio durante l'attivazione dell'app.
- Richiesta per l'aggiunta di Kaspersky Endpoint Security for Android all'elenco delle app eseguite all'avvio del sistema operativo (in alcuni dispositivi, come Huawei, Meizu e Xiaomi). Se la richiesta non viene visualizzata, aggiungere manualmente Kaspersky Endpoint Security for Android all'elenco delle app di avvio. La richiesta potrebbe non essere visualizzata se l'app di protezione non è installata nel profilo di lavoro.

È possibile concedere le autorizzazioni necessarie nella console EMM prima di distribuire l'app Kaspersky Endpoint Security for Android. Per maggiori informazioni sulla concessione delle autorizzazioni nella console EMM, visitare il *sito Web dell'assistenza tecnica del fornitore del servizio EMM*. È inoltre possibile concedere le autorizzazioni durante il completamento della Configurazione iniziale guidata di Kaspersky Endpoint Security for Android nel dispositivo.

L'app Kaspersky Endpoint Security for Android verrà installata nel profilo lavoro Android.

Per l'esecuzione di Protezione Web, è inoltre necessario configurare un server proxy nelle impostazioni di Google Chrome:

- Modalità di configurazione del server proxy: manuale.
- Porta e indirizzo server proxy: 127.0.0.1:3128.
- Supporto del protocollo SPDY: disabilitato.
- Compressione dei dati tramite il server proxy: disabilitata.

Come attivare l'app

Le informazioni sulla licenza vengono trasmesse al dispositivo mobile insieme alle altre impostazioni nel file di configurazione.

Se l'applicazione non viene attivata entro 30 giorni dall'installazione nel dispositivo mobile, la licenza di prova scadrà. Allo scadere della licenza di prova, tutte le funzionalità dell'app mobile Kaspersky Endpoint Security for Android vengono disabilitate.

Dopo la scadenza della licenza commerciale, l'app mobile continua a essere eseguita con funzionalità limitate (ad esempio, gli aggiornamenti dei database di Kaspersky Endpoint Security for Android non sono disponibili). Per continuare a utilizzare l'app con funzionalità complete, è necessario rinnovare la licenza commerciale.

Per attivare Kaspersky Endpoint Security for Android:

1. Nella console EMM aprire le impostazioni dell'app Kaspersky Endpoint Security for Android.
2. Nel campo `LicenseActivationCode` immettere il codice di attivazione dell'app.

   Per attivare l'app in un dispositivo, è necessario disporre dell'accesso ai server di attivazione Kaspersky.

Come connettere un dispositivo a Kaspersky Security Center

In seguito all'installazione di Kaspersky Endpoint Security for Android in un dispositivo mobile, è possibile connettere il dispositivo a Kaspersky Security Center. I dati necessari per connettere il dispositivo a Kaspersky Security Center vengono trasmessi al dispositivo mobile insieme alle altre impostazioni elencate nel file di configurazione. In seguito alla connessione del dispositivo a Kaspersky Security Center è possibile utilizzare i criteri di gruppo per configurare a livello centralizzato le impostazioni dell'app. È inoltre possibile ricevere rapporti e statistiche sulle prestazioni di Kaspersky Endpoint Security for Android.

Prima di connettere i dispositivi a Kaspersky Security Center, assicurarsi che siano soddisfatte le seguenti condizioni:

- Il plug-in di amministrazione di Kaspersky Endpoint Security for Android è installato nella workstation dell'amministratore.
- La porta per la connessione dei dispositivi mobili è aperta nelle proprietà di Administration Server.
- La visualizzazione della cartella **Mobile Device Management** è abilitata in Administration Console.
- Un certificato generale per l'identificazione dell'utente del dispositivo mobile è stato creato nell'archivio certificati di Kaspersky Security Center.

Prima di connettere i dispositivi a Kaspersky Security Center, è consigliabile eseguire le seguenti operazioni:

- Se si desidera creare attività e criteri per i dispositivi mobili, creare un gruppo di amministrazione separato per i dispositivi mobili.
- Se si desidera spostare automaticamente i dispositivi mobili in un gruppo di amministrazione separato, creare una regola per lo spostamento automatico dei dispositivi dalla cartella **Dispositivi non assegnati**.
- Se si desidera configurare a livello centralizzato Kaspersky Endpoint Security for Android, creare un criterio di gruppo.

Per connettere un dispositivo a Kaspersky Security Center:

1. Nella console EMM aprire le impostazioni dell'app Kaspersky Endpoint Security for Android.
2. Nel campo `KscServer` immettere il nome DNS o l'indirizzo IP di Kaspersky Security Center Administration Server. La porta predefinita è la numero 13292.
3. Se si desidera che l'utente non venga distratto dalle notifiche di Kaspersky Endpoint Security for Android, disabilitare le notifiche dell'app. A tale scopo, specificare l'impostazione `DisableNotification = True`.

   In seguito alla connessione, l'app visualizza tutte le notifiche. È possibile disabilitare le notifiche di determinate app nelle impostazioni dei criteri.

Non disabilitare le notifiche delle app se non si utilizza Kaspersky Security Center. In caso contrario l'utente potrebbe non ricevere le notifiche sulla scadenza della licenza. Di conseguenza, l'app smetterà di funzionare.

In seguito alla configurazione delle impostazioni di connessione, Kaspersky Endpoint Security for Android visualizza una notifica che richiede di concedere le seguenti autorizzazioni e i seguenti diritti aggiuntivi:

- Autorizzazione per l'utilizzo della fotocamera per il funzionamento di Antifurto (comando **Foto utente**).
- Autorizzazione per l'utilizzo della localizzazione per il funzionamento di Antifurto (comando **Localizza dispositivo**).
- Diritti di amministratore del dispositivo (proprietario del profilo lavoro Android) per l'esecuzione delle seguenti funzioni dell'app:
  - Installazione del certificato di sicurezza.
  - Configurazione del Wi-Fi.
  - Configurazione di Exchange ActiveSync.
  - Limitazione dell'utilizzo di fotocamera, Bluetooth e Wi-Fi.

A causa delle caratteristiche specifiche di un profilo lavoro Android (assenza del servizio Accessibilità), le funzioni Controllo app e Antifurto non sono disponibili nell'app.

Quando l'utente concede le autorizzazioni e i diritti necessari, il dispositivo si connetterà a Kaspersky Security Center. Se non è stata creata una regola per lo spostamento automatico dei dispositivi in un gruppo di amministrazione, il dispositivo verrà aggiunto automaticamente alla cartella **Dispositivi non assegnati**. Se è stata creata una regola per lo spostamento automatico dei dispositivi in un gruppo di amministrazione, il dispositivo verrà aggiunto automaticamente al gruppo definito.

Kaspersky Endpoint Security prevede il seguente formato dei nomi dei dispositivi:

- Modello dispositivo [e-mail, ID dispositivo]
- Modello dispositivo [e-mail (se presente) o ID dispositivo]

Un ID dispositivo è un ID univoco generato da Kaspersky Endpoint Security for Android a partire dai dati ricevuti da un dispositivo. Per i dispositivi mobili che eseguono Android 10 o versione successiva, Kaspersky Endpoint Security for Android utilizza il SSAID (ID Android) o il checksum di altri dati ricevuti dal dispositivo. Per le versioni precedenti di Android, l'app utilizza l'IMEI. È possibile configurare il formato dei nomi dei dispositivi nel criterio di gruppo. È inoltre possibile aggiungere un tag al nome del dispositivo. In questo modo è più semplice individuare e ordinare i dispositivi in Kaspersky Security Center. Il tag è disponibile solo per VMware AirWatch.

Per aggiungere il tag al nome del dispositivo:

1. Nella console EMM aprire le impostazioni dell'app Kaspersky Endpoint Security for Android.
2. Nel campo `KscDeviceNameTag` selezionare i valori:
   - `{DeviceSerialNumber}`: numero di serie del dispositivo.
   - `{DeviceUid}`: identificatore univoco del dispositivo.

- `{DeviceAssetNumber}`: numero di risorsa del dispositivo. Questo numero viene creato internamente nell'organizzazione.

> È consigliabile utilizzare soltanto questi valori. VMware AirWatch supporta altri valori, ma Kaspersky Endpoint Security non può garantire il funzionamento di tali valori.

È possibile aggiungere alcuni valori (ad esempio `{DeviceSerialNumber} {DeviceUid}`). Il tag verrà aggiunto al nome del dispositivo in Kaspersky Security Center. Il tag e il nome del dispositivo sono separati da uno spazio. Se ad esempio il nome del dispositivo è `Google Pixel 2 a10c6b75f7b31de9 22:7D:78:9E:C5:1E`, `22:7D:78:9E:C5:1E` è il tag identificatore univoco del dispositivo. Se si utilizzano Kaspersky Security Center e VMwareAirWatch, il tag consente di identificare i dispositivi in entrambe le console. Per la corrispondenza con il dispositivo, selezionare gli stessi valori per il nome del dispositivo (ad esempio il numero di serie del dispositivo).

In seguito alla connessione del dispositivo a Kaspersky Security Center, le impostazioni dell'app verranno modificate in base al criterio di gruppo. Kaspersky Endpoint Security for Android ignora le impostazioni dell'app presenti nel file di configurazione configurato nella console EMM. È possibile configurare tutte le sezioni del criterio ad eccezione delle seguenti sezioni:

- **Antifurto** (Blocco dispositivo)
- **Contenitori**
- **Gestione dispositivo** (Blocco schermo)
- **Controllo app** (Blocca le app vietate)
- **Profilo lavoro Android**
- **Gestisci Samsung KNOX**

> A causa del metodo utilizzato per distribuire un profilo lavoro, non è possibile applicare le impostazioni dei criteri di gruppo della sezione **Profilo lavoro Android**. Queste impostazioni possono essere applicate solo se il profilo lavoro è stato creato utilizzando Kaspersky Security Center.

File AppConfig

Viene generato un file di configurazione per configurare l'app in una console EMM. Le impostazioni dell'app nel file di configurazione sono presentate nella tabella seguente.

Impostazioni del file di configurazione

Chiave di configurazione	Descrizione	Tipo	Valore
`LicenseActivationCode`	Codice di attivazione dell'app	String	Il codice di attivazione dell'app è form da 20 caratteri dell'alfabeto latino e numeri. Per attivare l'app con un codi di attivazione, è necessario l'accesso Internet per connettersi ai server di attivazione Kaspersky.

			Se si lascia vuoto il campo, l'app verrà attivata con una licenza di prova. La licenza di prova ha una validità di 30 giorni. Allo scadere della licenza di pro tutte le funzionalità dell'app mobile Kaspersky Endpoint Security for And vengono disabilitate. Per continuare a utilizzare l'app, è necessario acquistar una licenza commerciale.
`EulaAcceptanceConfirmationV1`	<collegamento del Contratto di licenza>	Choice	Questa impostazione è disponibile solo per VMware AirWatch. `Accepted` – Confermo di aver letto, compreso e accettato i termini e le condizioni del presente Contratto di licenza con l'utente finale. `Declined` – Non accetto i termini e l condizioni del presente Contratto di licenza con l'utente finale (EULA). Per accettare i termini e le condizioni Contratto di licenza con l'utente final per tutti i dispositivi mobili, è necessa l'accesso a Internet per eseguire la connessione ai server Kaspersky. Se si sceglie `Declined`, l'app richiede all'utente di accettare i termini e le condizioni del Contratto di licenza co l'utente finale. Gli utenti dei dispositiv mobili possono accettare le condizion nella Configurazione iniziale guidata.
`EulaAcceptanceCodeV1`	Codice del Contratto di licenza	String	Queste impostazioni sono disponib solo per VMware AirWatch. Utilizzare `EulaAcceptanceCodeV1` s desidera accettare un singolo Contra di licenza con l'utente finale (EULA). Utilizzare `EulaAcceptanceCodesV2` si desidera accettare più Contratti di licenza con l'utente finale contemporaneamente. Il campo `EulaAcceptanceCodesV2` deve contenere un elenco di codici EULA separati da punto e virgola: `"<EULAid1>;<EULAid2>;<EULAid3>;..."`. Il codice del Contratto di licenza è contenuto nel Contratto di licenza co l'utente finale. *Per conoscere il codice del Contratto licenza:*
`EulaAcceptanceCodesV2`	Codici dei Contratti di licenza	String	

			1. Copiare il collegamento del Contratto di licenza (`EulaAcceptanceConfirmatior` dalla Console EMM. 2. Incollare il collegamento nel brows Viene aperto il Contratto di licenz con l'utente finale (EULA). 3. Leggere i termini e le condizioni de presente Contratto di licenza con l'utente finale e trovare il codice d Contratto di licenza. Per accettare i termini e le condizi dei Contratti di licenza con l'utent finale per tutti i dispositivi mobili, è necessario l'accesso a Internet pe eseguire la connessione ai server Kaspersky. Se i campi vengono lasciati vuoti, l'ap richiederà all'utente di accettare i ter e le condizioni dei Contratti di licenza con l'utente finale. L'utente del dispositivo mobile può accettare le condizioni nella Configurazione inizial guidata. Se si specificano i valori di entrambi i campi, verranno accettati i termini e l condizioni di tutti i Contratti di licenz con l'utente finale specificati.
`KscServer`	Indirizzo e porta di Kaspersky Security Center Administration Server	String	Nome DNS o indirizzo IP di Kaspersky Security Center Administration Serve numero di porta. Immettere l'indirizzo come segue: `<indirizzo server> <porta>`. Se si immette l'indirizzo del server senza specificare la porta, l'ap utilizzerà la porta predefinita 13292.
`DisableNotification`	Disabilitare le notifiche delle app prima della connessione a Kaspersky Security Center	Boolean	`True`: Kaspersky Endpoint Security f Android nasconde le notifiche di tutt app. Kaspersky Endpoint Security for Android nasconde le notifiche fino all connessione del dispositivo a Kasper Security Center. In seguito alla connessione, l'app visualizza tutte le notifiche. È possibile disabilitare le notifiche di determinate app nelle impostazioni dei criteri.

			Non disabilitare le notifiche delle app se non si utilizza Kaspersky Security Center. In caso contrario l'utente potrebbe non ricevere le notifiche sulla scadenza di una licenza. In questo caso l'app smetterebbe di eseguire le relative funzioni. `False`: Kaspersky Endpoint Security Android mostra le notifiche di tutte le app.

`ScanScheduleType`	Modalità esecuzione scansione	Choice	`AfterUpdate`: avviare una scansione virus dopo un aggiornamento dei database. L'app aggiorna i database a virus in base alla pianificazione definit (`UpdateScheduleType`).
			
			`Daily`: avviare una scansione virus u volta al giorno. Configurare l'ora di avv della scansione (`ScanScheduleTime`
			
			`Weekly`: avviare una scansione virus volta alla settimana. Selezionare il gio della settimana per l'avvio di una scansione virus (`ScanScheduleDay`) configurare l'ora (`ScanScheduleTim`
			
			`Off`: l'avvio automatico di una scansio virus è disabilitato.
			
			Indipendentemente dal valore impost l'utente del dispositivo può avviare manualmente una scansione virus.

`ScanScheduleDay`	Giorno per la scansione	Choice	`Monday / Tuesday / Wednesday Thursday / Friday / Saturday Sunday` È possibile selezionare un solo valore questa impostazione.
`ScanScheduleTime`	Ora per la scansione	String	L'ora può essere indicata nel formato ore (ad esempio, 13:00) o 12 ore (ad esempio, 10:30 PM).
`ScanScheduleLock`	Bloccare la configurazione della modalità di esecuzione della scansione	Boolean	`True`: l'utente non può accedere alle impostazioni della modalità di esecuzione della scansione virus nelle impostazioni dell'app. `False`: l'utente può configurare la modalità di esecuzione della scansion virus e, ad esempio, disabilitare l'avvio automatico di una scansione virus.
`ScanOnlyExecutableFiles`	Tipi di file per la scansione (scansione virus)	Choice	`AllFiles`: scansione di tutti i file. `OnlyExecutables`: scansione solo d file eseguibili. I file eseguibili sono file estensione APK (ZIP), DEX o SO.

			In Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1 non è possibile abilitare la scansione dei soli file eseguibili.
`ScanArchives`	Scansione degli archivi con decompressione	Boolean	`True`: l'app decomprime gli archivi e r esamina il contenuto. `False`: l'app esamina solo i file di archivio. L'app esamina solo gli archivi con estensione ZIP (APK). In Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1 non è possibile disabilitare la scansione dei contenuti degli archivi.
`ScanActionOnThreatFound`	Azione se viene rilevata una minaccia (scansione virus)	Choice	`Quarantine`: l'app mette gli oggetti rilevati in Quarantena. I file vengono memorizzati in Quarantena sotto forr di archivi, in modo che non possano danneggiare il dispositivo. Quarantena consente di eliminare o ripristinare i fi che sono stati spostati in un archivio isolato. `Delete`: l'app elimina gli oggetti rileva `Skip`: l'app non esegue alcuna azione sugli oggetti rilevati. Se gli oggetti rile sono stati ignorati, Kaspersky Endpoi Security for Android avvisa l'utente d problemi di protezione del dispositivo Quando si verifica un tentativo di accedere a un oggetto nel dispositivo (ad esempio, un tentativo di copiarlo aprirlo), l'app blocca l'accesso all'ogge `AskUser`: l'app richiede all'utente di selezionare un'azione per ogni oggett rilevato: ignorare, mettere in quarante o eliminare. Quando vengono rilevati p oggetti, l'utente può applicare un'azio selezionata a tutti gli oggetti. Le informazioni sulle minacce rilevate azioni eseguite su di esse vengono registrate nei rapporti dell'app.
`ScanLock`	Bloccare la configurazione delle impostazioni di scansione	Boolean	`True`: le seguenti impostazioni di scansione non sono accessibili da par dell'utente nelle impostazioni dell'app tipo di file da esaminare, scansione de archivi e azione da eseguire quando viene rilevata una minaccia. `False`: l'utente può configurare le impostazioni di scansione e, ad esemp selezionare l'azione `Skip` per le minac rilevate.
`ScanAndProtectionAdwareRiskware`	Blocca adware, autodialer e app che possono	Boolean	`True`: l'app rileva l'adware e altre app possono essere utilizzati da utenti

	essere utilizzati da utenti malintenzionati per danneggiare il dispositivo e i dati dell'utente		malintenzionati per danneggiare il dispositivo o i dati dell'utente. `False`: l'app ignora l'adware e altre ap che possono essere utilizzati da uten malintenzionati per danneggiare il dispositivo o i dati dell'utente.
`ProtectionMode`	Modalità di protezione in tempo reale	Choice	`Recommended`: l'app esamina una sola volta le nuove app subito dopo l'installazione, nonché i file nella carte Download. `Extended`: l'app esamina tutti i file aperti, modificati, copiati, eseguiti e salvati dall'utente nel dispositivo. L'ap esamina anche le nuove app e i file ne cartella Download. `Disabled`: protezione in tempo reale disabilitata.
`UseKsnMode`	Modalità Kaspersky Security Network	Choice	`Recommended`: l'app scambia dati cor Kaspersky Security Network (KSN). Kaspersky Endpoint Security for And utilizza KSN per la protezione in temp reale del dispositivo dalle minacce (Protezione cloud) e l'esecuzione di Protezione Web su Internet. `Extended`: l'app scambia dati con Kaspersky Security Network e invia anche al Virus Lab determinate statistiche sulle prestazioni di Kasper Endpoint Security for Android. Quest informazioni rendono possibile tenere traccia delle minacce in tempo reale. Tramite i servizi KSN non vengono raccolti, elaborati o memorizzati dati personali. `Disabled`: l'app non utilizza i dati di Kaspersky Security Network. Non è possibile abilitare Protezione Web (`EnableWebFilter`). Il componente Protezione cloud non è disponibile pe Anti-Virus.
`ProtectScanOnlyExecutableFiles`	Tipi di file per la scansione (protezione in tempo reale)	Boolean	`AllFiles`: scansione di tutti i file. `OnlyExecutables`: scansione solo d file eseguibili. I file eseguibili sono file estensione APK (ZIP), DEX o SO. In Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 1 non è possibile abilitare la scansione dei soli file eseguibili.
`ProtectionActionOnThreatFound`	Azione se viene rilevata una minaccia (protezione in tempo reale)	Choice	`Quarantine`: l'app mette gli oggetti rilevati in Quarantena. I file vengono memorizzati in Quarantena sotto forr di archivi, in modo che non possano danneggiare il dispositivo. Quarantena

			consente di eliminare o ripristinare i fi che sono stati spostati in un archivio isolato. `Delete`: l'app elimina gli oggetti rileva `Skip`: l'app non esegue alcuna azione sugli oggetti rilevati. Se gli oggetti rile sono stati ignorati, Kaspersky Endpoi Security for Android avvisa l'utente d problemi di protezione del dispositivo Quando viene effettuato un tentativo accedere a un oggetto nel dispositivo (ad esempio un tentativo di copiarlo o aprirlo), l'app blocca l'accesso all'ogge Le informazioni sulle minacce rilevate azioni eseguite su di esse vengono registrate nei rapporti dell'app.
`ProtectionLock`	Bloccare la configurazione delle impostazioni di protezione in tempo reale	Boolean	`True`: le seguenti impostazioni di protezione in tempo reale non sono accessibili da parte dell'utente nelle impostazioni dell'app: modalità di protezione in tempo reale, tipi di file p la scansione e azione da eseguire quando viene rilevata una minaccia. `False`: l'utente può configurare le impostazioni di protezione in tempo r e, ad esempio, selezionare l'azione `Sk` per le minacce rilevate.
`UpdateScheduleType`	Modalità esecuzione aggiornamento dei database	Choice	`Daily`: verificare la disponibilità di nu database anti-virus e scaricarli nei dispositivi una volta al giorno. Configurare l'ora di avvio dell'aggiornamento dei database (`UpdateScheduleTime`). `Weekly`: verificare la disponibilità di nuovi database anti-virus e scaricarli dispositivi una volta alla settimana. Selezionare il giorno della settimana p l'avvio di un aggiornamento dei datab (`UpdateScheduleDay`) e configurare l'ora (`UpdateScheduleTime`). `Off`: l'aggiornamento automatico dei database anti-virus è disabilitato. Indipendentemente dal valore impost l'utente può avviare manualmente l'aggiornamento dei database anti-vir
`UpdateScheduleDay`	Giorno per l'avvio di un aggiornamento dei database	Choice	`Monday / Tuesday / Wednesday Thursday / Friday / Saturday Sunday` È possibile selezionare un solo valore questa impostazione.
`UpdateScheduleTime`	Ora di avvio dell'aggiornamento dei database	String	L'ora può essere indicata nel formato ore (ad esempio, 13:00) o 12 ore (ad esempio, 10:30 PM).

`UpdateScheduleLock`	Bloccare la configurazione della modalità di esecuzione dell'aggiornamento dei database	Boolean	`True`: l'utente non può accedere alle impostazioni della modalità di esecuzione dell'aggiornamento dei database nelle impostazioni dell'app. `False`: l'utente può configurare la modalità di esecuzione dell'aggiornamento dei database e, ad esempio, disabilitare l'avvio automatico degli aggiornamenti dei database anti-virus.
`AllowUpdateInRoaming`	Aggiornare i database in roaming	Boolean	`True`: l'app scarica i database anti-virus se il dispositivo si trova nell'area di roaming. L'app scarica i database anti-virus in base alla pianificazione definita (`UpdateScheduleType`). `False`: l'app scarica i database anti-virus solo se il dispositivo si trova nella rete principale.

`EnableWebFilter`	Protezione Web	Boolean	`True`: l'app utilizza il componente Protezione Web per bloccare i siti Web dannosi e di phishing su Internet. Protezione Web supporta solo Google Chrome.
			I siti Web dannosi e di phishing che utilizzano il protocollo HTTPS possono rimanere sbloccati se il dominio è attendibile. Se il dominio non è attendibile, Protezione Web blocca i siti Web dannosi e di phishing.
			`False`: la protezione contro i siti Web dannosi e di phishing è disabilitata.
			Per l'utilizzo del componente Protezione Web, devono essere soddisfatte le seguenti condizioni:
			• Gli utenti dei dispositivi accettano l'Informativa sulla privacy e l'Informativa di Protezione Web nella Configurazione iniziale guidata o nelle impostazioni dell'app.
			• Un server proxy è configurato nelle impostazioni del browser:
			`ProxyMode = "fixed_servers"`
			`ProxyServer = "127.0.0.1:3128"`
			`DisableSpdy = true`
			`DataCompressionProxyEnabled = false`

			La configurazione del server proxy può variare in base alla versione di Google Chrome. Per maggiori informazioni sulla configurazione d Google Chrome, visitare il sito We del progetto Chromium. Dopo la rimozione dell'app Kasper Endpoint Security for Android dal dispositivo mobile, reimpostare le impostazioni del server proxy. • L'utilizzo di KSN è abilitato nelle impostazioni dell'app: `UseKsnMod` `Recommended` o `UseKsnMode = Extended`. • È consigliabile selezionare Google Chrome come browser predefinit nelle impostazioni del sistema operativo.
`EnableWebFilterLock`	Bloccare la configurazione di Protezione Web	Boolean	`True`: l'utente non può accedere alle impostazioni di Protezione Web nelle impostazioni dell'app. `False`: l'utente può configurare le impostazioni di Protezione Web e, ad esempio, disabilitare la protezione co i siti Web dannosi e di phishing su Internet.
`UpdateServer`	Indirizzo del server di origine degli aggiornamenti dei database	String	Indirizzo del server che contiene il database degli aggiornamenti, ad esempio `http://update.server.c` Se si lascia vuoto il campo, Kaspersky Endpoint Security for Android utilizza server di aggiornamento database di Kaspersky.
`AllowGoogleAnalytics`	Inviare i dati ai servizi Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics	Boolean	`True`: l'app invia automaticamente i d sull'esecuzione di Kaspersky Endpoint Security for Android ai servizi Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics. Questi dati sono necessari per migliorare le prestazioni dell'app e analizzare la soddisfazione degli utenti. I dati veng trasferiti ai servizi Google Analytics p Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics tramite una connessione sicura. L'accesso ai dati e la relativa protezione sono disciplinati dalle condizioni di utilizzo dei servizi Googl Analytics per Firebase, Attestazione SafetyNet Firebase Performance Monitoring e Crashlytics.

			`False`: l'invio di dati ai servizi Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics è disabilitato
`KscDeviceNameTag`	Tag del nome dispositivo per Kaspersky Security Center	String	Questa impostazione è disponibile solo per VMware AirWatch. Il tag verrà aggiunto al nome del dispositivo in Kaspersky Security Center. Il tag e il nome del dispositivo sono separati da uno spazio. In questo modo è più semplice individuare e ordinare i dispositivi in Kaspersky Security Center. • `{DeviceSerialNumber}`: numero serie del dispositivo. • `{DeviceUid}`: identificatore univ del dispositivo. • `{DeviceAssetNumber}`: numero risorsa del dispositivo. Questo numero viene creato internamente nell'organizzazione. È possibile aggiungere alcuni valori (ad esempio `{DeviceSerialNumber}` `{DeviceUid}`). È consigliabile utilizzare soltanto questi valori. VMware AirWatch supporta altri valori, ma Kaspersky Endpoint Security non può garantir il funzionamento di tali valori.
`KscGroup`	Nome del gruppo di dispositivi	String	È possibile specificare i gruppi di dispositivi in una console EMM. Quand un dispositivo è connesso a Kaspersky Security Center, verrà automaticamente aggiunto a una sottocartella della cartella Dispositivi non assegnati. Il no della sottocartella corrisponderà al no del gruppo specificato in questo parametro. È quindi possibile creare regole per lo spostamento automatico dei dispositivi dalle sottocartelle della cartella Dispositivi non assegnati ai gruppi di amministrazione nella cartella Dispositivi gestiti.

			Se il campo viene lasciato vuoto, il dispositivo verrà automaticamente aggiunto alla radice della cartella Dispositivi non assegnati.
`KscCorporateEmail`	Indirizzo e-mail aziendale dell'utente	String	È possibile specificare gli indirizzi e-m aziendali degli utenti in una console E Questi indirizzi e-mail verranno visualizzati in Kaspersky Security Cer La stringa deve essere un indirizzo e- valido. Gli altri valori vengono ignorati.

Carico di rete

Questa sezione contiene informazioni sul volume del traffico di rete scambiato tra i dispositivi mobili e Kaspersky Security Center.

Volume del traffico

Attività	Traffico in uscita	Traffico in entrata	Traffico totale
Distribuzione iniziale dell'app, MB	0,08	17,76	17,84
Aggiornamento iniziale dei database anti-virus (il volume di traffico può variare a seconda delle dimensioni dei database anti-virus), MB	0,04	2,21	2,25
Sincronizzazione del dispositivo mobile con Kaspersky Security Center, MB	0,03	0,02	0,05
Aggiornamento periodico dei database anti-virus (il volume di traffico può variare a seconda delle dimensioni dei database anti-virus), MB	0,08	3,06	3,14
Esecuzione dei comandi di Antifurto. Localizza dispositivo (il volume di traffico può variare a seconda delle specifiche della fotocamera incorporata e della qualità delle immagini), MB	0,09	0,8	0,17
Esecuzione dei comandi di Antifurto. Foto utente, MB	1,0	0,02	1,02
Esecuzione dei comandi di Antifurto. Blocco Dispositivo, MB	0,06	0,05	0,11
Volume giornaliero medio, MB	0,22	6,96	7,18

Partecipazione a Kaspersky Security Network

Per proteggere i dispositivi mobili più efficacemente, Kaspersky Endpoint Security for Android utilizza dati acquisiti da utenti di tutto il mondo. L'elaborazione di questi dati viene eseguita tramite *Kaspersky Security Network*.

Kaspersky Security Network (KSN) è un'infrastruttura di servizi cloud che consente l'accesso alla Knowledge Base online di Kaspersky con informazioni sulla reputazione di file, risorse Web e software. L'utilizzo dei dati provenienti da Kaspersky Security Network garantisce una risposta più rapida da parte delle applicazioni Kaspersky alle nuove minacce, migliora le prestazioni di alcuni componenti di protezione e riduce la probabilità di falsi allarmi.

La partecipazione a Kaspersky Security Network consente a Kaspersky di acquisire informazioni in tempo reale sui tipi e sulle origini delle nuove minacce, sviluppare metodi per la loro neutralizzazione e ridurre il numero di falsi allarmi in Kaspersky Endpoint Security for Android. La partecipazione a Kaspersky Security Network consente inoltre di accedere alle statistiche sulla reputazione di applicazioni e siti Web.

Quando si partecipa a Kaspersky Security Network, alcune statistiche vengono acquisite durante l'esecuzione di Kaspersky Endpoint Security for Android e vengono inviate automaticamente a Kaspersky. Queste informazioni rendono possibile tenere traccia delle minacce in tempo reale. I file o le relative parti che possono essere sfruttati da utenti malintenzionati per danneggiare il computer o i contenuti dell'utente possono anche essere inviati a Kaspersky per essere sottoposti a un'ulteriore analisi.

L'utilizzo di Kaspersky Security Network è obbligatorio per il funzionamento di Kaspersky Endpoint Security for Android. KSN è utilizzato dai componenti principali dell'app: Anti-Virus, Protezione Web e Controllo app. Il rifiuto di partecipare a KSN comporta la riduzione del livello di protezione del dispositivo, che può provocare l'infezione del dispositivo e la perdita dei dati. Per iniziare a utilizzare Kaspersky Security Network, è necessario accettare i termini del Contratto di licenza con l'utente finale durante l'installazione dell'app. Leggendo il Contratto di licenza con l'utente finale, è possibile scoprire quali dati vengono trasmessi a Kaspersky Security Network da Kaspersky Endpoint Security for Android.

Per migliorare le prestazioni dell'app, è possibile fornire dati statistici aggiuntivi a Kaspersky Security Network. L'inserimento delle informazioni sopra indicate nel sistema KSN è facoltativo. Per iniziare a utilizzare Kaspersky Security Network, è necessario accettare le condizioni di uno speciale contratto: *l'Informativa di Kaspersky Security Network*. È possibile scegliere di interrompere la partecipazione a Kaspersky Security Network in qualsiasi momento. L'Informativa di Kaspersky Security Network descrive i tipi di dati trasmessi da Kaspersky Endpoint Security for Android a Kaspersky Security Network.

Scambio di informazioni con Kaspersky Security Network

Per migliorare la protezione in tempo reale, Kaspersky Security for Mobile utilizza il servizio cloud Kaspersky Security Network per l'esecuzione dei seguenti componenti:

- **Anti-Virus.** L'app ottiene accesso alla Knowledge Base online di Kaspersky, con informazioni sulla reputazione di file e app. La scansione viene eseguita per le minacce per cui non sono state ancora aggiunte informazioni ai database anti-virus, ma che sono già disponibili in KSN. Il servizio cloud di Kaspersky Security Network garantisce l'esecuzione completa di Anti-virus e riduce la probabilità di falsi allarmi.

- **Protezione Web.** L'app utilizza i dati ricevuti da KSN per eseguire una scansione dei siti Web prima dell'apertura. L'app determina inoltre la categoria del sito Web per controllare l'accesso a Internet degli utenti in base agli elenchi delle categorie consentite e bloccate (ad esempio, la categoria "Comunicazioni di rete").

- **Controllo app.** L'app determina la categoria dell'app per limitare l'avvio delle app che non soddisfano i requisiti di sicurezza aziendali in base agli elenchi delle categorie consentite e bloccate (ad esempio, la categoria "Giochi").

Le informazioni sul tipo di dati inviati a Kaspersky durante l'utilizzo di KSN con Anti-Virus e Controllo app sono disponibili nel Contratto di licenza con l'utente finale. Accettando i termini e le condizioni del Contratto di licenza, si accetta il trasferimento di queste informazioni.

Le informazioni sul tipo di dati inviati a Kaspersky durante l'utilizzo di KSN con Protezione Web sono disponibili nell'Informativa relativa all'elaborazione dei dati per Protezione Web. Accettando i termini e le condizioni dell'Informativa, si accetta il trasferimento di queste informazioni.

Allo scopo di rilevare le minacce emergenti per la sicurezza delle informazioni, le intrusioni e le minacce difficili da rilevare (insieme alle relative origini) e migliorare la protezione delle informazioni archiviate ed elaborate in un dispositivo, è possibile estendere la propria partecipazione a Kaspersky Security Network.

Per consentire lo scambio dei dati con KSN al fine di migliorare le prestazioni dell'app, devono essere soddisfatte le seguenti condizioni:

- L'utente in questione o l'utente del dispositivo deve leggere e accettare i termini dell'Informativa di Kaspersky Security Network. Se si opta per l'accettazione dell'Informativa da parte degli utenti, a questi ultimi verrà richiesto di accettare i termini dell'Informativa tramite una notifica nella schermata principale dell'app. Gli utenti possono inoltre accettare le informative nella sezione **Informazioni sull'app** presente nelle impostazioni di Kaspersky Endpoint Security for Android.

  Se si sceglie di accettare le informative a livello globale, le versioni delle informative accettate tramite Kaspersky Security Center devono corrispondere alle versioni già accettate dagli utenti. In caso contrario, gli utenti verranno informati del problema e verrà loro richiesto di accettare la versione di un'informativa corrispondente alla versione accettata a livello globale dall'amministratore. Anche lo stato del dispositivo nel plug-in di Kaspersky Security for Mobile (Devices) diventerà *Avviso*.

- È necessario configurare le impostazioni del criterio di gruppo per consentire l'invio delle statistiche a KSN.

È possibile scegliere di interrompere l'invio di dati statistici a Kaspersky Security Network in qualsiasi momento. Le informazioni sul tipo di dati statistici inviati a Kaspersky durante l'utilizzo di KSN con l'app mobile Kaspersky Endpoint Security for Android sono disponibili nell'Informativa di Kaspersky Security Network.

Per ulteriori informazioni sulla trasmissione dei dati a KSN, fare riferimento alla sezione "Trasmissione dei dati".

La trasmissione dei dati a KSN è volontaria. Se lo si desidera, è possibile disabilitare lo scambio dei dati con KSN.

Abilitazione e disabilitazione dell'utilizzo di Kaspersky Security Network

Per l'esecuzione dei componenti di Kaspersky Endpoint Security for Android che utilizzano Kaspersky Security Network, l'app invia richieste ai servizi cloud. Le richieste contengono i dati come descritto nella sezione "Trasmissione dei dati".

Se l'utilizzo di Kaspersky Security Network è disabilitato nel dispositivo, i componenti Protezione Cloud, Protezione Web e Controllo app sono disabilitati automaticamente.

Per abilitare o disabilitare l'utilizzo di Kaspersky Security Network:

1. Aprire la finestra con le impostazioni del criterio di gestione per i dispositivi mobili in cui è installato Kaspersky Endpoint Security for Android.
2. Nella finestra **Proprietà** del criterio selezionare la sezione **Avanzate**.
3. Nella sezione **Impostazioni di Kaspersky Security Network (KSN)** configurare le impostazioni per l'utilizzo di Kaspersky Security Network:
   - Selezionare la casella **Usa Kaspersky Security Network** per l'esecuzione dei seguenti componenti: Anti-Virus (Protezione cloud), Protezione Web e Controllo app (categorie di app).
   - Selezionare la casella **Consentire l'invio delle statistiche a KSN** per inviare i dati a Kaspersky. L'utilizzo di questi dati garantisce una risposta più rapida alle nuove minacce da parte dell'app Kaspersky Endpoint Security for Android, migliora le prestazioni dei componenti di protezione e riduce la probabilità di falsi allarmi.
4. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. Una volta applicato il criterio, i componenti che utilizzano Kaspersky Security Network sono disabilitati e le impostazioni dei componenti diventano non disponibili.

Utilizzo di Kaspersky Private Security Network

Kaspersky Private Security Network (di seguito denominato anche *KSN Privato* o *KPSN)* è una soluzione che garantisce l'accesso ai database di reputazione di Kaspersky Security Network, senza l'invio dei dati dai dispositivi degli utenti a Kaspersky Security Network.

Un database delle reputazioni degli oggetti (file o URL) è archiviato nel server Kaspersky Private Security Network, ma non nei server Kaspersky Security Network. I database di reputazione KPSN sono archiviati nella rete aziendale e vengono gestiti dall'amministratore dell'azienda.

Quando KPSN è abilitato, Kaspersky Endpoint Security non invia dati statistici dai dispositivi degli utenti a KSN.

Per abilitare l'utilizzo di KSN Privato tramite Kaspersky Security Center:

1. Fare clic su **Impostazioni** ( ) nella finestra principale di Kaspersky Security Center Web Console o Cloud Console.

   Verrà visualizzata la finestra delle proprietà di Administration Server.

2. Nella scheda **Generale** selezionare la sezione **Impostazioni proxy KSN.**

3. Spostare l'interruttore sulla posizione **Usa Kaspersky Private Security Network ABILITATO**.

4. Fare clic sul pulsante **Seleziona file con impostazioni proxy KSN**, quindi cercare il file di configurazione con estensione pkcs7 o pem (fornita da Kaspersky).

5. Fare clic su **Apri**.

6. Se le impostazioni del server proxy sono configurate nelle proprietà di Administration Server, ma l'architettura di rete richiede l'utilizzo diretto di KSN Privato, abilitare l'opzione **Ignora impostazioni del server proxy KSC durante la connessione a KSN Privato**. In caso contrario, le richieste provenienti dalle applicazioni gestite non possono raggiungere KSN Privato.

7. Fare clic sul pulsante **Salva**.

Dopo aver scaricato le impostazioni, l'interfaccia mostra il nome e i contatti del fornitore, nonché la data di creazione del file con le impostazioni di KSN Privato. Le impostazioni di KPSN verranno applicate ai dispositivi mobili.

Quando si passa a KSN Privato, Controllo app non supporta le categorie di app disponibili durante l'utilizzo di KSN Globale. La categorizzazione delle app sarà disponibile se si sceglie di tornare a KSN.

Trasmissione dei dati a servizi di terze parti

Kaspersky Endpoint Security for Android utilizza i servizi Google™ noti come Firebase Cloud Messaging, Google Analytics per Firebase™, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics. Kaspersky Endpoint Security for Android utilizza il servizio FCM (Firebase Cloud Messaging) per garantire l'invio tempestivo dei comandi ai dispositivi mobili e la sincronizzazione forzata quando le impostazioni dei criteri vengono modificate. Kaspersky Endpoint Security for Android utilizza i servizi Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics per migliorare le prestazioni dell'app e per consentire a Kaspersky di creare materiali di marketing più efficaci.

Scambio di informazioni con Firebase Cloud Messaging

Kaspersky Endpoint Security for Android utilizza il servizio FCM (Firebase Cloud Messaging) per garantire l'invio tempestivo dei comandi ai dispositivi mobili e la sincronizzazione forzata quando le impostazioni dei criteri vengono modificate. L'app utilizza inoltre le notifiche push.

Per utilizzare il servizio Firebase Cloud Messaging, è necessario configurare le impostazioni del servizio in Kaspersky Security Center. Per maggiori informazioni sulla configurazione di Firebase Cloud Messaging in Kaspersky Security Center, fare riferimento alla *Guida di Kaspersky Security Center*. Se le impostazioni di Firebase Cloud Messaging non sono configurate, i comandi nel dispositivo mobile e le impostazioni dei criteri verranno inviati quando il dispositivo viene sincronizzato con Kaspersky Security Center in base alla pianificazione impostata nel criterio (ad esempio, ogni 24 ore). In altre parole, i comandi e le impostazioni dei criteri verranno inviati con un ritardo.

Allo scopo di supportare la funzionalità principale del prodotto, si accetta di fornire automaticamente il servizio Firebase Cloud Messaging con l'ID univoco dell'installazione dell'app (ID istanza) e i seguenti dati:

- Informazioni sul software installato: versione dell'app, ID dell'app, versione della build dell'app, nome del pacchetto dell'app.
- Informazioni sul computer in cui è installato il software: versione del sistema operativo, ID dispositivo, versione dei servizi Google.
- Informazioni su FCM: ID dell'app in FCM, ID utente di FCM, versione del protocollo.

I dati vengono trasmessi ai servizi Firebase tramite una connessione sicura. L'accesso alle e la protezione delle informazioni sono disciplinati dalle relative condizioni di utilizzo del servizio Firebase: https://firebase.google.com/terms/data-processing-terms/, https://firebase.google.com/support/privacy/.

Per impedire lo scambio di informazioni con il servizio Firebase Cloud Messaging:

1. Nella struttura della console selezionare **Mobile Device Management** → **Dispositivi mobili**.
2. Nel menu di scelta rapida della cartella **Dispositivi mobili** selezionare **Proprietà**.
3. Nella finestra delle proprietà della cartella **Dispositivi mobili** selezionare la sezione **Impostazioni di Google Firebase Cloud Messaging**.
4. Fare clic sul pulsante **Ripristina impostazioni**.

Scambio di informazioni con Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics

Se si utilizza il plug-in di amministrazione di una versione precedente ed è stato abilitato lo scambio dei dati con il servizio Google Analytics, Kaspersky Endpoint Security for Android Service Pack 4 Maintenance Release 3 eseguirà lo scambio dei dati con il servizio Google Analytics per Firebase. Il supporto di Google Analytics è stato sospeso.

Kaspersky Security for Mobile esegue lo scambio dei dati con i servizi Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics per le seguenti finalità:

- Per migliorare le prestazioni dell'app.

  Per consentire lo scambio dei dati con i servizi Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics al fine di migliorare le prestazioni dell'app, devono essere soddisfatte le seguenti condizioni:

  - L'amministratore o l'utente del dispositivo deve leggere e accettare i termini dell'Informativa di Kaspersky Security Network. Se si opta per l'accettazione dell'Informativa da parte degli utenti, a questi ultimi verrà richiesto di accettare i termini dell'Informativa tramite una notifica nella schermata principale dell'app. Gli utenti possono inoltre accettare le informative nella sezione **Informazioni sull'app** presente nelle impostazioni di Kaspersky Endpoint Security for Android.

    Se si sceglie di accettare le informative a livello globale, le versioni delle informative accettate tramite Kaspersky Security Center devono corrispondere alle versioni già accettate dagli utenti. In caso contrario, gli utenti verranno informati del problema e verrà loro richiesto di accettare la versione di un'informativa corrispondente alla versione accettata a livello globale dall'amministratore. Anche lo stato del dispositivo nel plug-in di Kaspersky Security for Mobile (Devices) diventerà *Avviso*.

  - L'amministratore deve configurare le impostazioni del criterio di gruppo per consentire l'invio delle statistiche a KSN (vedere di seguito).

- Per consentire a Kaspersky di creare materiali di marketing più efficaci.

  Per consentire lo scambio dei dati con i servizi Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics al fine di supportare Kaspersky nella creazione di materiali di marketing efficaci, devono essere soddisfatte le seguenti condizioni:

  - L'amministratore o l'utente del dispositivo deve leggere e accettare i termini dell'Informativa relativa all'elaborazione dei dati per finalità di marketing. Se si opta per l'accettazione dell'Informativa da parte degli utenti, questi potranno accettare i termini dell'Informativa durante l'installazione dell'app o nella sezione **Informazioni sull'app** presente nelle impostazioni di Kaspersky Endpoint Security for Android.

  - L'amministratore deve configurare le impostazioni del criterio di gruppo per consentire l'invio dei dati a Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics (vedere di seguito).

[Trasmissione dei dati a Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics nell'ambito dell'Informativa relativa all'elaborazione dei dati per finalità di marketing]

Il Titolare dei diritti utilizza sistemi informatici di terze parti per elaborare i dati. Le modalità di trattamento dei dati di tali sistemi sono disciplinate dalle rispettive dichiarazioni sulla privacy. Di seguito sono elencati i servizi di cui si avvale il Titolare dei diritti e i dati da essi elaborati:

Google Analytics per Firebase

Durante l'utilizzo del Software, i seguenti dati verranno trasmessi automaticamente e regolarmente a Google Analytics per Firebase per lo scopo dichiarato:

- Informazioni sull'app (versione e ID dell'app, ID dell'app nel servizio Firebase, ID istanza nel servizio Firebase, nome dello store da cui è stata scaricata l'applicazione, data e ora del primo avvio del Software)
- ID di installazione dell'app nel dispositivo e metodo di installazione nel dispositivo
- Informazioni sull'area geografica e sulla lingua
- Informazioni sulla risoluzione dello schermo del dispositivo
- Informazioni sull'utente che ha ottenuto la root
- Informazioni di diagnostica sul dispositivo dal servizio SafetyNet Attestation
- Informazioni sull'impostazione di Kaspersky Endpoint Security for Android come funzione di accessibilità.
- Informazioni sulle transizioni fra schermate dell'applicazione, durata delle sessioni, inizio e fine di una sessione della schermata, nome della schermata
- Informazioni sul protocollo utilizzato per inviare i dati al servizio Firebase, la versione e l'ID del metodo di invio utilizzato
- Dettagli sul tipo e i parametri dell'evento per cui vengono inviati i dati
- Informazioni sulla licenza dell'app, la disponibilità e il numero di dispositivi
- Informazioni sulla frequenza degli aggiornamenti del database anti-virus e sulla sincronizzazione con Administration Server
- Informazioni sulla console di amministrazione (Kaspersky Security Center o sistemi EMM di terze parti)
- ID Android
- ID inserzionista
- informazioni sull'Utente: fascia d'età e sesso, identificativo del paese di residenza ed elenco di interessi
- informazioni sul computer dell'Utente in cui è installato il Software: nome del produttore del computer, tipo di computer, modello, versione e lingua (impostazioni locali) del sistema operativo, informazioni sull'applicazione aperta per la prima volta negli ultimi 7 giorni e sull'applicazione aperta per la prima volta più di 7 giorni fa

  I dati vengono trasmessi a FireBase tramite un canale protetto. Le informazioni sul trattamento dei dati da parte di Firebase sono disponibili su: https://firebase.google.com/support/privacy.

Attestazione SafetyNet

Durante l'utilizzo del Software, i seguenti dati verranno trasmessi automaticamente e regolarmente all'attestazione SafetyNet per lo scopo dichiarato:

- ora del controllo dispositivo
- informazioni sul software, nome e data dei certificati software
- risultati del controllo dispositivo
- controlli casuali dell'ID per verificare il risultati del dispositivo di controllo

  I dati vengono inoltrati all'attestazione SafetyNet tramite un canale protetto. Le informazioni sul trattamento dei dati da parte di SafetyNet Attestation sono disponibili su: https://policies.google.com/privacy.

Monitoraggio delle prestazioni di Firebase

Durante l'utilizzo del Software, i seguenti dati verranno trasmessi automaticamente e regolarmente a Firebase Performance Monitoring per lo scopo dichiarato:

- ID di installazione univoco
- nome pacchetto applicazioni
- versione del software installato
- livello della batteria e stato di carica della batteria
- operatore
- stato dell'app in primo piano o in background
- geografia
- Indirizzo IP
- codice lingua dispositivo
- informazioni sulla connessione di rete/via radio
- ID istanza Software pseudonimo
- RAM e dimensioni del disco
- contrassegno indicante se il dispositivo è collegato a un rooter o se è stato manomesso con jailbreak
- potenza del segnale
- durata delle tracce automatiche
- rete e le seguenti informazioni corrispondenti: codice di risposta, dimensioni payload in byte, tempo di risposta
- descrizione del dispositivo

  I dati vengono trasmessi a Firebase Performance Monitoring tramite un canale protetto. Le informazioni sul trattamento dei dati da parte di Firebase Performance Monitoring sono disponibili all'indirizzo: https://firebase.google.com/support/privacy.

Crashlytics

Durante l'utilizzo del Software, i seguenti dati verranno trasmessi automaticamente e regolarmente a Crashlytics per lo scopo dichiarato:

- ID software
- versione del software installato
- contrassegno indicante se il Software era in esecuzione in background
- architettura della CPU
- ID evento univoco
- data e ora dell'evento
- modello dispositivo
- spazio totale sul disco e quantità attualmente utilizzata
- nome e versione del sistema operativo
- RAM totale e quantità attualmente utilizzata
- contrassegno indicante se il dispositivo è collegato a un rooter
- orientamento dello schermo all'ora dell'evento
- prodotto/produttore hardware
- ID di installazione univoco
- versione delle statistiche inviate
- tipo di eccezione del Software
- testo del messaggio di errore
- un contrassegno indicante che l'eccezione del Software è stata causata da un'eccezione nidificata
- ID thread
- un contrassegno indicante se il frame è stato la causa dell'errore del Software
- un contrassegno indicante che il thread ha causato l'arresto imprevisto del Software
- informazioni sul segnale che ha causato l'arresto imprevisto del Software: nome del segnale, codice del segnale, indirizzo del segnale
- per ogni frame associato a un thread, un'eccezione o un errore: il nome del file di frame, il numero di riga del file di frame, i simboli di debug, l'indirizzo e l'offset nell'immagine binaria, il nome visualizzato della raccolta con il frame, il tipo di frame, il contrassegno indicante se il frame è stato la causa dell'errore
- ID sistema operativo
- ID del problema associato all'evento

- informazioni sugli eventi che si sono verificati prima che il Software si arrestasse in modo imprevisto: identificatore dell'evento, data e ora dell'evento, tipo e valore dell'evento;
- valori di registro CPU;
- tipo e valore dell'evento.

  I dati vengono inoltrati a Crashlytics tramite un canale protetto. Le informazioni sul trattamento dei dati da parte di Crashlytics sono disponibili su: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

La fornitura delle suddette informazioni a scopo di trattamento per finalità di marketing è volontaria.

Per disabilitare lo scambio dei dati con i servizi Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics:

1. Aprire la finestra di configurazione del criterio di gestione per i dispositivi mobili in cui è installata l'app Kaspersky Endpoint Security for Android.
2. Nella finestra **Proprietà** del criterio selezionare la sezione **Avanzate**.
3. Nella sezione **Trasferimento dei dati** deselezionare la casella di controllo **Consenti il trasferimento dei dati per aiutare a migliorare la qualità, l'aspetto e le prestazioni dell'app**.
4. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Accettazione globale di informative aggiuntive

Per abilitare la protezione fornita da Kaspersky Endpoint Security for Android, è necessario accettare i termini del Contratto di licenza con l'utente finale, nonché informative aggiuntive (vedere di seguito). Configurare un criterio per accettare le informative elencate di seguito a livello globale per tutti gli utenti. Agli utenti non verrà richiesto di leggere e accettare i termini dei seguenti contratti e informative che sono già stati accettati a livello globale:

- Informativa di Kaspersky Security Network
- Informativa relativa all'elaborazione dei dati per Protezione Web
- Informativa relativa all'elaborazione dei dati per finalità di marketing

Se si sceglie di accettare le informative a livello globale, le versioni delle informative accettate tramite Kaspersky Security Center devono corrispondere alle versioni già accettate dagli utenti. In caso contrario, gli utenti verranno informati del problema e verrà loro richiesto di accettare la versione di un'informativa corrispondente alla versione accettata a livello globale dall'amministratore. Anche lo stato del dispositivo nel plug-in di Kaspersky Security for Mobile (Devices) diventerà *Avviso*.

Per scegliere se i termini devono essere accettati a livello globale o dagli utenti applicando un criterio di gruppo:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Avanzate**.
5. Nella sezione **Trasferimento dati** scegliere se l'Informativa relativa all'elaborazione dei dati per finalità di marketing sarà accettata a livello globale o dagli utenti.
6. Nella sezione **Impostazioni di Kaspersky Security Network (KSN)** scegliere se l'Informativa di Kaspersky Security Network sarà accettata a livello globale o dagli utenti.
7. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

L'utente può accettare i termini di un'informativa o rifiutarli in qualsiasi momento nella sezione **Informazioni sull'app** nelle impostazioni di Kaspersky Endpoint Security for Android.

Samsung KNOX

Samsung KNOX è una soluzione mobile per la configurazione e la protezione dei dispositivi mobili Samsung che eseguono il sistema operativo Android. Per maggiori informazioni su Samsung KNOX, visitare il *sito Web dell'assistenza tecnica di Samsung*.

Installazione dell'app Kaspersky Endpoint Security for Android tramite KNOX Mobile Enrollment

KNOX Mobile Enrollment (KME) fa parte della soluzione mobile Samsung KNOX. Viene utilizzato per l'installazione in batch e la configurazione iniziale delle app nei nuovi dispositivi Samsung acquistati da fornitori ufficiali.

L'installazione dell'app Kaspersky Endpoint Security for Android tramite KNOX Mobile Enrollment è costituita dai seguenti passaggi:

1. **Creazione di un profilo MDM KNOX con l'app Kaspersky Endpoint Security for Android.**
2. **Aggiunta di dispositivi in KNOX Mobile Enrollment.**
3. **Installazione dell'app Kaspersky Endpoint Security for Android nei dispositivi mobili dell'utente.**

Per maggiori informazioni sull'utilizzo di KNOX Mobile Enrollment, fare riferimento al *Manuale dell'utente di KNOX Mobile Enrollment*.

La distribuzione tramite KNOX Mobile Enrollment è possibile solo per i dispositivi Samsung. Per l'elenco dei dispositivi supportati, visitare il *sito Web dell'assistenza tecnica di Samsung*.

Creazione di un profilo MDM KNOX

Un profilo *MDM KNOX* è un profilo che contiene collegamenti alle app per la distribuzione rapida e la configurazione iniziale nei dispositivi mobili.

Per creare un profilo MDM KNOX:

1. Accedere alla console Samsung KNOX → **KNOX Mobile Enrollment**.
2. Selezionare la sezione **MDM profiles (Profili MDM)**.
3. Fare clic su **Aggiungi**.

   Verrà avviata la creazione guidata del nuovo profilo MDM KNOX.
4. Nel passaggio **MDM server connection (Connessione al server MDM)** selezionare **Server URI is not required for my MDM service (Server URI non richiesto per il servizio MDM)** e fare clic su **Avanti**.
5. Nel passaggio **MDM profile info (Informazioni sul profilo MDM)**:
   a. Immettere le informazioni generali sul profilo MDM KNOX: **Profile name (Nome profilo)** e **Descrizione**.
   b. Fare clic sul pulsante **Add MDM apps (Aggiungi app MDM)** e immettere il percorso del file di installazione APK.

      Il file di installazione per Kaspersky Endpoint Security for Android è incluso nel kit di distribuzione di Kaspersky Security for Mobile. Prima di tutto posizionare il file di installazione APK nel Server Web di Kaspersky Security Center o in un altro server accessibile per il download dal dispositivo.
   c. Immettere le impostazioni per la connessione del dispositivo a Kaspersky Security Center nel campo **JSON user data (Dati utente JSON)** nel seguente formato:
   `{"serverAddress":"ksc.server.com","serverPort":"12345","groupName":"MOBILE GROUP"}`.

      Il dispositivo deve essere connesso a Kaspersky Security Center per poter attivare l'app, configurare il dispositivo e inviare comandi.
   d. Selezionare la casella di controllo **Add Knox agreements (Aggiungi contratti Knox)**.

      Per installare Kaspersky Endpoint Security for Android tramite KNOX Mobile Enrollment, l'utente del dispositivo mobile deve accettare i termini del Contratto di licenza Samsung. È possibile visualizzare i termini del Contratto di licenza Samsung nella sezione denominata **End User License Agreements, Terms of Service, and User Agreements (Contratti di licenza con l'utente finale, Termini di servizio e Contratti con l'utente)**. È inoltre possibile aggiungere altri documenti legali dell'azienda che sono necessari per la distribuzione di un profilo MDM KNOX facendo clic sul pulsante **Add user agreement (Aggiungi contratto con l'utente)**.
   e. Deselezionare la licenza **Bind Knox license to this profile (Associa licenza Knox a questo profilo)**.

      Le informazioni sulla licenza Samsung KNOX vengono distribuite al dispositivo mobile insieme al criterio quando il dispositivo viene sincronizzato con Kaspersky Security Center.
6. Fare clic sul pulsante **Salva**.

Di conseguenza, il nuovo profilo MDM KNOX con l'app Kaspersky Endpoint Security for Android verrà aggiunto all'elenco nella console KME.

Aggiunta di dispositivi in KNOX Mobile Enrollment

I dispositivi possono essere aggiunti nella console KNOX Mobile Enrollment (KME) nei seguenti modi:

- Il fornitore aggiunge automaticamente i dispositivi nella console KME dopo l'acquisto dei dispositivi.

  Selezionare questo metodo se l'organizzazione collabora con un fornitore ufficiale di dispositivi Samsung.

- L'amministratore installa l'app KNOX Deployment da Google Play nel dispositivo mobile ed esegue la migrazione del profilo MDM KNOX nei dispositivi degli utenti tramite Bluetooth o NFC (Near Field Communication). Dopo la distribuzione del profilo MDM KNOX, il dispositivo verrà automaticamente aggiunto nella console KME.

  Selezionare questo metodo se i dispositivi Samsung non sono stati acquistati da un fornitore ufficiale.

Aggiunta di un dispositivo tramite il fornitore

I fornitori ufficiali di dispositivi Samsung sono registrati in Samsung KNOX. Per l'elenco dei fornitori ufficiali, visitare il *sito Web dell'assistenza tecnica di Samsung*. Il fornitore aggiunge automaticamente i dispositivi nella console KME per l'account Samsung subito dopo l'acquisto dei dispositivi. Per fare in modo che i dispositivi vengano aggiunti dal fornitore, è necessario registrare il fornitore nella console KME per l'account Samsung. Per aggiungere il fornitore di dispositivi Samsung nella console KME sarà necessario un ID rivenditore. Per ricevere l'ID rivenditore, è necessario inviare una richiesta al fornitore. Nella richiesta specificare l'ID client KNOX.

Per visualizzare l'ID client KNOX:

1. Accedere alla console Samsung KNOX → **KNOX Mobile Enrollment**.
2. Selezionare la sezione **Resellers (Rivenditori)**.
3. L'ID viene visualizzato nel campo **KNOX client ID (ID client KNOX)**.

Dopo la ricezione di una risposta dal fornitore con l'ID rivenditore, registrare il fornitore nella console KME. Prima della registrazione del fornitore, è possibile creare un profilo MDM KNOX in modo che il profilo venga automaticamente distribuito durante l'aggiunta di nuovi dispositivi.

Per registrare un fornitore ufficiale nella console KME:

1. Accedere alla console Samsung KNOX → **KNOX Mobile Enrollment**.
2. Selezionare la sezione **Resellers (Rivenditori)**.
3. Fare clic sul pulsante **Register reseller (Registra rivenditore)**.

   Verrà visualizzata una finestra per registrare il fornitore del dispositivo.
4. Nel campo **Reseller ID (ID rivenditore)** immettere l'ID ricevuto dal fornitore ufficiale di dispositivi Samsung.
5. Se è stato creato un profilo MDM KNOX, selezionare il profilo MDM KNOX nella finestra di registrazione del fornitore.

   Quando si aggiungono nuovi dispositivi, il profilo MDM KNOX viene installato automaticamente.
6. Nell'elenco **Preferred download confirmation method (Metodo di conferma del download preferito)** selezionare un metodo per confermare l'aggiunta di un dispositivo per un fornitore.

   - **All downloads must be confirmed (Tutti i download devono essere confermati)**. Quando un dispositivo viene aggiunto dal fornitore, sarà necessario confermare l'operazione.
   - **Automatically confirm all downloads of this reseller (Conferma automaticamente tutti i download di questo rivenditore)**. I dispositivi del fornitore verranno automaticamente aggiunti nella console KME.
7. Fare clic su **OK**.

Il fornitore di dispositivi Samsung verrà aggiunto all'elenco dei fornitori nella console KME.

In seguito all'acquisto di nuovi dispositivi dal fornitore ufficiale, l'app Kaspersky Endpoint Security for Android verrà automaticamente installata nei dispositivi dopo che questi ultimi si connettono a Internet. Per maggiori informazioni sull'utilizzo di KNOX Mobile Enrollment, fare riferimento al *Manuale dell'utente di KNOX Mobile Enrollment*. Se si dispone già di un elenco di dispositivi nella console KME, aggiungere il profilo MDM KNOX con l'app MDM KNOX nel dispositivo.

Per distribuire un profilo MDM KNOX nei dispositivi:

1. Accedere alla console Samsung KNOX → **KNOX Mobile Enrollment**.
2. Selezionare **Devices (Dispositivi)** → **All devices (Tutti i dispositivi)**.
3. Selezionare i dispositivi in cui si desidera installare il profilo MDM KNOX.
4. Fare clic sul pulsante **Configure (Configura)**.

   Verrà visualizzata la finestra **Device info (Informazioni dispositivo)**.
5. Nell'elenco **MDM profile (Profilo MDM)**, selezionare il profilo MDM KNOX con l'app Kaspersky Endpoint Security for Android.
6. Nel campo **Tags (Tag)** immettere i tag per raggruppare ed etichettare i dispositivi, nonché per l'ottimizzazione delle ricerche nella console KME.
7. Immettere le credenziali dell'account utente del dispositivo nei campi **User ID (ID utente)** e **Password**.

   Le credenziali dell'account sono richieste per la ricezione di un certificato generale. L'ID utente e la password devono corrispondere alle credenziali dell'account utente in Kaspersky Security Center (Nome completo e Password nelle proprietà dell'account utente).
8. Selezionare il profilo MDM KNOX per i dispositivi rimanenti.
9. Fare clic sul pulsante **Salva**.

Dopo la connessione del dispositivo a Internet, all'utente verrà richiesto di installare il profilo MDM KNOX.

Aggiunta di un dispositivo tramite l'app KNOX Deployment

Se il dispositivo Samsung non è stato acquistato da un fornitore ufficiale, è possibile aggiungere il dispositivo a KNOX Mobile Enrollment tramite Bluetooth o NFC. Questo richiederà al dispositivo mobile dell'amministratore utilizzato di distribuire i profili MDM KNOX ai dispositivi mobili degli utenti.

Per aggiungere dispositivi utilizzando l'app KNOX Deployment, devono essere soddisfatte le seguenti condizioni:

- A seconda della modalità di distribuzione selezionata, i moduli Bluetooth o NFC devono essere abilitati nei dispositivi mobili.
- I dispositivi mobili devono essere connessi a Internet.

Per distribuire un profilo MDM KNOX utilizzando l'app KNOX Deployment:

1. Installare l'app KNOX Deployment da Google Play nel dispositivo mobile dell'amministratore.
2. Avviare l'app KNOX Deployment.
3. Immettere le credenziali dell'account Samsung.

4. Nella finestra **KNOX Deployment** configurare le impostazioni per distribuire un profilo MDM KNOX:

   - Selezionare il profilo MDM KNOX.
   - Selezionare la modalità di distribuzione: **Bluetooth** o **NFC**.

     Se si utilizza Bluetooth, è possibile aggiungere un profilo MDM KNOX in più dispositivi contemporaneamente.

5. Fare clic su **Start deployment (Avvia distribuzione)**:

   - **Bluetooth**. Nel dispositivo mobile dell'utente aprire il sito Web https://configure.samsungknox.com.

     Verrà avviata la procedura guidata di registrazione dei dispositivi Samsung KNOX. Seguire le istruzioni visualizzate.

     Dopo l'installazione del profilo MDM KNOX, il nuovo dispositivo con il tag **Bluetooth** verrà aggiunto nella console KME.

   - **NFC**. Avvicinare il dispositivo mobile dell'amministratore al dispositivo mobile dell'utente e trasferire il profilo MDM KNOX.

     Nel dispositivo mobile dell'utente verrà visualizzata una richiesta di installazione del profilo MDM KNOX. Il nuovo dispositivo con il tag **NFC** verrà aggiunto nella console KME.

Installazione dell'app

Prima di installare l'app Kaspersky Endpoint Security for Android, emettere un certificato generale per gli utenti dei dispositivi mobili in Kaspersky Security Center Administration Console. È richiesto un certificato generale per identificare l'utente del dispositivo mobile in Kaspersky Security Center Administration Console.

Dopo la distribuzione del profilo MDM KNOX, il file di installazione APK verrà automaticamente scaricato nel dispositivo mobile. L'installazione dell'app Kaspersky Endpoint Security for Android viene avviata automaticamente. L'utente deve accettare il Contratto di licenza di Samsung KNOX e il Contratto di licenza di Kaspersky Endpoint Security for Android. Non è richiesta una configurazione aggiuntiva dell'app. Dopo l'installazione dell'app, la sincronizzazione con Kaspersky Security Center verrà eseguita automaticamente. Il dispositivo mobile verrà aggiunto a Kaspersky Security Center Administration Console nel gruppo di amministrazione specificato nelle impostazioni del profilo MDM KNOX (`groupName`).

Configurazione dei contenitori KNOX

Questa sezione contiene informazioni sull'utilizzo dei contenitori KNOX nei dispositivi Samsung che eseguono Android.

L'utilizzo dei contenitori KNOX è disponibile solo nei dispositivi Samsung con sistema operativo Android 6.0 o versione successiva.

Informazioni sui contenitori KNOX

Un *contenitore KNOX* è un ambiente sicuro nel dispositivo di un utente con desktop, riquadro di avvio, app e widget specifici. Un contenitore KNOX consente di isolare le app e i dati aziendali da quelli personali. Un contenitore KNOX è un componente della soluzione mobile Samsung KNOX.

Samsung KNOX è una soluzione mobile per la configurazione e la protezione dei dispositivi mobili Samsung che eseguono il sistema operativo Android. Per maggiori informazioni su Samsung KNOX, visitare il *sito Web dell'assistenza tecnica di Samsung*.

I contenitori KNOX consentono di separare dati personali e aziendali in un dispositivo mobile. Ad esempio, è impossibile utilizzare una cassetta postale personale per inviare un file che si trova in un contenitore KNOX. È consigliabile distribuire un contenitore KNOX se i dispositivi mobili personali dei dipendenti vengono utilizzati per l'utilizzo dei dati aziendali.

Per utilizzare contenitori KNOX, è necessario attivare Samsung KNOX. Dopo la sincronizzazione di un dispositivo con Kaspersky Security Center, all'utente del dispositivo mobile verrà richiesto di installare il contenitore KNOX. Prima di installare il contenitore KNOX, l'utente deve accettare le condizioni del Contratto di licenza con l'utente finale di Samsung.

Dopo l'installazione del contenitore KNOX, l'icona KNOX verrà aggiunta al desktop del dispositivo mobile. In alternativa l'area di lavoro verrà aggiunta all'elenco delle app nel dispositivo mobile. Per l'utilizzo dei dati aziendali, l'utente deve avviare l'app dal contenitore KNOX.

Kaspersky Endpoint Security for Android non è installato nel contenitore KNOX e non protegge i dati aziendali. Kaspersky Endpoint Security for Android non rileva il download di file dannosi e blocca i siti dannosi nel contenitore KNOX. Non è possibile controllare l'avvio delle app o vietare l'uso della fotocamera nel contenitore KNOX. Kaspersky Endpoint Security for Android protegge solo i dati privati. È possibile proteggere i dati aziendali con gli strumenti Samsung KNOX. Per maggiori informazioni su Samsung KNOX, visitare il *sito Web dell'assistenza tecnica di Samsung*.

Attivazione di Samsung KNOX

Per utilizzare un contenitore KNOX nel dispositivo mobile dell'utente, è necessario attivare Samsung KNOX. La procedura di attivazione di Samsung KNOX dipende dalla versione di Kaspersky Endpoint Security for Android installata nei dispositivi degli utenti:

- Se nei dispositivi è installata la versione corrente di Kaspersky Endpoint Security for Android, non sono necessarie chiavi per attivare Samsung KNOX.
- Se nei dispositivi è installata una versione precedente di Kaspersky Endpoint Security for Android (10.8.3.174 o versione precedente), è necessario ottenere una chiave KNOX License Manager (di seguito denominata chiave KLM) da Samsung. La *chiave di gestione delle licenze KNOX* è un codice univoco utilizzato dal sistema di gestione delle licenze Samsung KNOX. Per informazioni dettagliate sulla chiave KLM, consultare il sito Web dell'assistenza tecnica Samsung KNOX.

L'utilizzo dei contenitori KNOX è possibile solo nei dispositivi Samsung.

Per attivare Samsung KNOX:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Gestisci Samsung KNOX → Contenitori KNOX**.

5. Nel campo **Chiave di gestione delle licenze KNOX** specificare quanto segue:

   - Se la versione corrente di Kaspersky Endpoint Security for Android è installata nei dispositivi, digitare un carattere qualsiasi.

   - Se nei dispositivi è installata una versione precedente di Kaspersky Endpoint Security for Android (10.8.3.174 o precedente), immettere la chiave KLM ricevuta da Samsung.

6. Impostare l'opzione lucchetto nella posizione bloccata .

7. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Samsung KNOX verrà attivato dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. All'utente verrà richiesto di accettare le condizioni del Contratto di licenza con l'utente finale di Samsung e di installare il contenitore KNOX.

Per disattivare Samsung KNOX:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.

3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.

4. Nella finestra **Proprietà** del criterio selezionare la sezione **Gestisci Samsung KNOX → Contenitori KNOX**.

5. Cancellare il valore del campo **Chiave di gestione delle licenze KNOX**.

6. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Samsung KNOX verrà disattivato dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center. L'accesso al contenitore KNOX verrà bloccato.

Limitazioni relative a Samsung KNOX

- L'utilizzo dei contenitori KNOX è disponibile solo nei dispositivi Samsung.

- Nei dispositivi Samsung che supportano KNOX 2.6, 2.7 e 2.7.1 Protezione Web e Controllo app non funzionano in un contenitore KNOX. Questo problema è correlato alla mancanza delle autorizzazioni richieste nel contenitore KNOX (servizio di accessibilità). Nei dispositivi che supportano KNOX 2.8 o versioni successive tutti i componenti dell'app funzionano senza limitazioni.

- Le versioni di Kaspersky Endpoint Security for Android precedenti a Service Pack 4 Maintenance Release 3 Update 2 potrebbero non funzionare in modo stabile nei dispositivi Samsung Android 10 a causa degli aggiornamenti Samsung KNOX. È consigliabile aggiornare Kaspersky Endpoint Security for Android alla versione Service Pack 4 Maintenance Release 3 Update 2.

Configurazione del firewall in KNOX

È necessario configurare le impostazioni del firewall per monitorare le connessioni di rete in un contenitore KNOX.

Per configurare il firewall in un contenitore KNOX:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.
2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Gestisci Samsung KNOX → Contenitori KNOX**.
5. Nella finestra **Firewall** fare clic su **Configura**.
   Verrà visualizzata la finestra **Firewall**.
6. Selezionare la modalità Firewall:
   - Per consentire tutte le connessioni in entrata e in uscita, spostare il cursore su **Consenti tutto**.
   - Per bloccare tutte le attività di rete tranne quelle delle app nell'elenco delle esclusioni, spostare il cursore su **Blocca tutto tranne le eccezioni**.
7. Se è stata impostata la modalità Firewall su **Blocca tutto tranne le eccezioni**, creare un elenco di esclusioni:
   a. Fare clic su **Aggiungi**.
      Verrà visualizzata la finestra **Esclusione per Firewall**.
   b. Nel campo **Nome app** immettere il nome di un'app mobile.
   c. Nel campo **Nome pacchetto** immettere il nome di sistema del pacchetto di app mobili (ad esempio `com.mobileapp.example`).
   d. Fare clic su **OK**.
8. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Configurazione di una cassetta postale Exchange in KNOX

Per utilizzare posta aziendale, contatti e calendario in un contenitore KNOX, è necessario configurare le impostazioni della cassetta postale Exchange.

Per configurare una cassetta postale Exchange in un contenitore KNOX:

1. Nella struttura della console, nella cartella **Dispositivi gestiti**, selezionare il gruppo di amministrazione a cui appartengono i dispositivi Android.

2. Nell'area di lavoro di un gruppo selezionare la scheda **Criteri**.
3. Aprire la finestra delle proprietà del criterio facendo doppio clic su una colonna.
4. Nella finestra **Proprietà** del criterio selezionare la sezione **Gestisci Samsung KNOX → Contenitori KNOX**.
5. Nella finestra **Exchange ActiveSync** fare clic sul pulsante **Configura**.
   Verrà visualizzata la finestra **Impostazioni server e-mail Exchange**.
6. Nel campo **Indirizzo server** immettere l'indirizzo IP o il nome DNS del server che ospita il server di posta.
7. Nel campo **Dominio** immettere il nome del dominio dell'utente del dispositivo mobile nella rete aziendale.
8. Nell'elenco a discesa **Intervallo di sincronizzazione** selezionare l'intervallo desiderato per la sincronizzazione del dispositivo mobile con il server Microsoft Exchange.
9. Per utilizzare il protocollo di trasporto dati SSL (Secure Sockets Layer), selezionare la casella **Usa connessione SSL**.
10. Per utilizzare certificati digitali per proteggere il trasferimento dei dati tra il dispositivo mobile e il server Microsoft Exchange, selezionare la casella **Verifica certificato server**.
11. Fare clic sul pulsante **Applica** per salvare le modifiche apportate.

Le impostazioni del dispositivo mobile vengono configurate dopo la successiva sincronizzazione del dispositivo con Kaspersky Security Center.

Appendici

Questa sezione fornisce informazioni complementari al testo del documento.

Autorizzazioni di configurazione dei criteri di gruppo

Gli amministratori di Kaspersky Security Center possono configurare i diritti di accesso degli utenti di Administration Console per le diverse funzioni dell'applicazione, a seconda delle mansioni degli utenti.

Per ogni area funzionale, l'amministratore può assegnare le seguenti autorizzazioni:

- **Consenti la modifica**. L'utente di Administration Console può modificare le impostazioni dei criteri nella finestra delle proprietà.
- **Blocca la modifica**. L'utente di Administration Console non può modificare le impostazioni dei criteri nella finestra delle proprietà. Le schede dei criteri che appartengono all'ambito funzionale per cui il diritto è stato assegnato non vengono visualizzate nell'interfaccia.

Autorizzazioni per l'accesso alle sezioni del plug-in di amministrazione di Kaspersky Endpoint Security

Ambito funzionale	Sezione dei criteri
Android Enterprise	Profilo lavoro Android
Antifurto	Antifurto
Controllo app	Controllo app

Protezione	Protezione, scansione, aggiornamento
Controllo conformità	Controllo conformità
Contenitori	Contenitori
Impostazioni dispositivo	Controllo dispositivi, sincronizzazione
Gestione dei dispositivi Samsung	APN, gestione dei dispositivi Samsung, contenitori KNOX
Gestione sistema	Avanzate, Wi-Fi
Protezione Web	Protezione Web

Autorizzazioni per l'accesso alle sezioni del plug-in di amministrazione di Kaspersky Device Management for iOS

Ambito funzionale	Sezione dei criteri
Avanzate	Clip Web, Caratteri, AirPlay, AirPrint
Exchange ActiveSync	Generale, Password, Sincronizzazione, Limitazioni delle funzionalità, Limitazioni delle applicazioni
Generale	Generale, Single Sign-On, Protezione Web, Wi-Fi, Nome punto di accesso (APN), Exchange ActiveSync, E-mail, Payload personalizzato
LDAP (calendario / contatti)	LDAP, Calendario, Contatti, Calendario sottoscritto
Limitazioni e sicurezza	Restrizione per le funzionalità, Restrizioni per le applicazioni, Limitazioni per i contenuti multimediali, Password, VPN, Proxy HTTP globale, Certificati, SCEP

Categorie di app

Controllo app supporta la classificazione delle app. La modalità di esecuzione configurata per la categoria di app è applicata a tutte le app in questa categoria. La categoria di ogni app è determinata dal servizio cloud Kaspersky Security Network.

Categorie di app

Categoria	Descrizione
Intrattenimento	App per l'intrattenimento interattivo.
Client IM, app di messaggistica mobili	App di messaggistica istantanea, comunicazione vocale e video tramite IP.
Social network	App per l'utilizzo di social network e blog.
Software aziendale	App per il calcolo delle imposte, gestione di operazioni bancarie, gestione di fogli di calcolo, contabilità e altre app orientate alle attività aziendali. Editor di testo.
Casa, famiglia, stile di vita, salute	App con ricette, suggerimenti di stile. App per esercizi, pianificazione di allenamenti, suggerimenti su diete, alimentazione sana, sicurezza e prevenzione degli infortuni.
Medicina	App con cataloghi di sintomi e cure, app per professionisti della sanità, riviste e notizie di assistenza sanitaria.
Elementi	Servizi per abbonamenti a film, lettori multimediali e lettori video. Servizi musicali, lettori,

multimediali	trasmissioni radio.
Software di progettazione grafica	App per l'utilizzo con una fotocamera, editor di immagini, app per la gestione e la pubblicazione di fotografie.
Plug-in per newsfeed e RSS	App per la lettura di giornali, riviste, blog e aggregatori di notizie.
Meteo	App che visualizzano previsioni meteorologiche.
Software educativo	Lettori di libri, manuali, libri di testo, dizionari, thesaurus, enciclopedie. App per la preparazione di esami, materiali di formazione, dizionari, giochi educativi, strumenti per lo studio di lingue straniere.
Acquisti online	App per acquisti online e la partecipazione ad aste, coupon regalo, strumenti per il confronto di prezzi, app per elenchi di acquisti, app per la lettura di feedback sui prodotti.
Utilità di avvio	App per la riprogettazione del desktop, widget, combinazioni di tasti.
Sistemi operativi e utilità	App di sistema che consentono la gestione del sistema operativo, l'interazione dell'utente e la gestione della RAM.
Visualizzatori mappe	Guide di città, informazioni su aziende locali, strumenti per la pianificazione di viaggi.
Altro software	Librerie di software, versioni demo tecniche di app. App non incluse in alcuna categoria.
Mezzi di trasporto	App per l'utilizzo di trasporti pubblici, strumenti di navigazione, app per guidatori.
Giochi	Arcade, scommesse, corse, altro, casinò, giochi di carte, musica, giochi da tavolo, guide, rompicapo, avventure, RPG, simulatori, giochi di parole, giochi di sport, strategia, azione.
Browser	App per la visualizzazione di siti Web, contenuti di documenti Web e file. App per la gestione di applicazioni Web.
Strumenti di sviluppo	App per lo sviluppo di software. Debugger, compilatori, editor di codice, editor di interfacce grafiche.
Software del sistema operativo	App fornite con il sistema operativo e richieste per il corretto funzionamento del sistema operativo.
Software Internet	Gestori di download, client di posta, app per la ricerca sul Web e altre app per l'esplorazione di Internet.
Software di infrastruttura di rete	App per la gestione dei server, dispositivi di archiviazione dei dati, attrezzature di rete, software per reti aziendali, automazione e integrazione dell'infrastruttura completa.
Software di rete	App per l'organizzazione della collaborazione di un gruppo di utenti su più dispositivi, comunicazione tra dispositivi.
Utilità di sistema	App fornite con il sistema operativo: gestori di file, strumenti di archiviazione, utilità per la diagnostica di hardware e software, strumenti di ottimizzazione della memoria, programmi di disinstallazione, utilità di gestione del processore.
Software di protezione	App di protezione dei dati nel dispositivo. App che rilevano e neutralizzano le minacce nel dispositivo. Firewall. App di criptaggio dei dati.
Download manager	App per il download di file da origini esterne.
Software di	App per la gestione dell'archiviazione online di file, note e contenuti multimediali.

archiviazione in Internet	
Software di riferimento	Lettori di libri, manuali, libri di testo, dizionari, thesaurus, enciclopedie e wiki.
Applicazioni e-mail	App utilizzate per l'invio e la ricezione di messaggi e-mail.

Utilizzo dell'app Kaspersky Endpoint Security for Android

Questa sezione della Guida descrive le funzionalità e le operazioni disponibili per gli utenti dell'app Kaspersky Endpoint Security for Android.

Gli articoli in questa sezione comprendono tutte le opzioni potenzialmente disponibili o visibili in un dispositivo mobile. Il layout e il comportamento effettivi dell'app dipendono dal sistema di amministrazione remota implementato e dal modo in cui l'amministratore configura il dispositivo in base ai requisiti di sicurezza aziendali. Alcune funzioni e opzioni descritte in questa sezione potrebbero non essere applicabili all'effettiva esperienza dell'utente relativa all'app. In caso di domande sull'app nel dispositivo specifico, contattare l'amministratore.

Funzionalità dell'app

Kaspersky Endpoint Security offre le seguenti funzionalità principali.

Protezione da virus e altro malware

L'app utilizza il componente Anti-Virus per proteggere il dispositivo da virus e altro malware.

Anti-Virus esegue le seguenti funzioni:

- Esegue la scansione delle minacce nell'intero dispositivo, nelle app installate o nelle cartelle selezionate
- Protegge il dispositivo in tempo reale
- Esegue la scansione delle nuove app installate prima che vengano avviate per la prima volta
- Aggiorna i database anti-virus

Se un'applicazione che si occupa della raccolta e dell'invio delle informazioni per l'elaborazione è installata in un dispositivo mobile, Kaspersky Endpoint Security for Android può classificare questa applicazione come malware.

Controllo app

In base ai requisiti di sicurezza aziendale, *l'amministratore del sistema di amministrazione remota* (di seguito denominato anche "amministratore") crea elenchi di app consigliate, bloccate e richieste. Il componente Controllo app viene utilizzato per installare e aggiornare le app consigliate e richieste e per rimuovere le app bloccate.

Controllo app consente di installare le app consigliate e richieste nel dispositivo tramite un collegamento diretto al pacchetto di distribuzione o tramite un collegamento a Google Play. Controllo app consente di rimuovere le app bloccate che violano i requisiti di sicurezza aziendali.

Kaspersky Endpoint Security deve essere abilitato come un servizio funzionalità di accessibilità al fine di garantire il corretto funzionamento di Controllo app. Se non è stato abilitato questo servizio durante l'esecuzione della procedura guidata di configurazione iniziale per l'app, è possibile abilitare Kaspersky Endpoint Security come servizio per le funzionalità di accessibilità nella sezione **Stato** selezionando la notifica appropriata oppure nelle impostazioni del dispositivo (**Impostazioni Android** → **Accessibilità** → **Servizi**).

Protezione dei dati di un dispositivo rubato o smarrito

Il componente Antifurto protegge i dati dagli accessi non autorizzati e consente di localizzare il dispositivo in caso di furto o smarrimento.

Antifurto consente di eseguire le seguenti operazioni in remoto:

- Bloccare il dispositivo.

  Per impedire a un hacker di sbloccare il dispositivo, Kaspersky Endpoint Security deve essere abilitato come servizio per le funzionalità di accessibilità nei dispositivi mobili che eseguono Android 7.0 o versione successiva.

- Attivare allarme sonoro nel dispositivo anche se l'audio del dispositivo è disabilitato.
- Ottenere le coordinate della posizione del dispositivo sulla mappa.
- Cancellare i dati archiviati nel dispositivo.
- Ripristina le impostazioni predefinite.
- Scattare di nascosto una foto utente della persona che sta utilizzando il dispositivo.

Per abilitare le operazioni di Antifurto, Kaspersky Endpoint Security deve essere abilitato come amministratore del dispositivo. Se non sono stati concessi i diritti di amministratore del dispositivo durante la configurazione iniziale delle app, è possibile concedere i diritti di amministratore a Kaspersky Endpoint Security nella sezione **Stato** selezionando la notifica appropriata oppure nelle impostazioni del dispositivo (**Impostazioni Android** → **Sicurezza** → **Amministratori dispositivo**).

Protezione dalle minacce online

Il componente Protezione Web garantisce la protezione dalle minacce online.

Protezione Web blocca i siti Web dannosi che distribuiscono codice dannoso e i siti Web di phishing progettati per rubare le informazioni riservate dell'utente e ottenere l'accesso ai conti personali. Protezione Web analizza i siti Web prima dell'apertura utilizzando il servizio cloud Kaspersky Security Network.

Per abilitare Protezione Web:

- Kaspersky Endpoint Security deve essere abilitato come servizio per le funzionalità di accessibilità.
- È necessario accettare l'Informativa relativa all'elaborazione dei dati a scopo di utilizzo di Protezione Web (Informativa di Protezione Web). Kaspersky Endpoint Security utilizza Kaspersky Security Network (KSN) per

eseguire la scansione dei siti Web. L'Informativa di Protezione Web contiene i termini dello scambio di dati con KSN.

L'amministratore può accettare l'Informativa di Protezione Web al posto dell'utente in Kaspersky Security Center. In questo caso non è necessario eseguire alcuna azione.

Se l'amministratore non ha accettato l'Informativa di Protezione Web e ha inviato la richiesta all'utente, è necessario leggere e accettare l'Informativa di Protezione Web nelle impostazioni dell'app.

Se l'amministratore non ha accettato l'Informativa di Protezione Web, Protezione Web non è disponibile.

Protezione Web nei dispositivi Android funziona solo nel browser Google Chrome (inclusa la funzionalità Schede personalizzate), in Huawei Browser e Samsung Internet Browser. Protezione Web per Samsung Internet Browser non blocca i siti su un dispositivo mobile se viene utilizzato un profilo lavoro e Protezione Web è abilitato solo per il profilo lavoro.

Descrizione della finestra principale

L'aspetto della finestra principale varia leggermente a seconda della risoluzione dello schermo.

L'aspetto della schermata principale cambia in caso di problemi che possono determinare una riduzione del livello di protezione, l'infezione del dispositivo o la perdita di informazioni.

La sezione **Stato** visualizza le seguenti informazioni:

- Problemi di protezione del dispositivo
- Informazioni sulla conformità o mancata conformità del dispositivo con i requisiti di sicurezza aziendali
- Informazioni sullo stato di protezione del dispositivo

La sezione **Stato** può essere aperta toccando la parte superiore della finestra principale di Kaspersky Endpoint Security.

Problemi di protezione del dispositivo

I problemi di protezione sono raggruppati per categorie. Per ogni problema sono elencate le azioni che è possibile eseguire per la risoluzione.

La sezione **Stato** visualizza inoltre un elenco degli oggetti ignorati rilevati dall'app. L'elenco degli oggetti ignorati può ad esempio cambiare se un file dannoso è stato eliminato o spostato. Per ricevere un elenco aggiornato delle minacce, eseguire una scansione completa del dispositivo. Per garantire la protezione ottimale dei dati, eliminare tutti gli oggetti rilevati.

Esistono due tipi di problemi di protezione:

- *Notifiche*. In giallo. Le notifiche informano l'utente degli eventi che possono compromettere la sicurezza del dispositivo, ad esempio il fatto che l'ultima scansione è stata eseguita più di 14 giorni fa o che non è stata eseguita la scansione di una nuova app installata. È possibile nascondere un problema di notifica. Successivamente è possibile accedere alle informazioni sul problema dal menu **Problemi nascosti**.

- *Problemi critici*. In rosso. I problemi critici segnalano all'utente gli eventi di importanza critica per la sicurezza del dispositivo, ad esempio il fatto che i database anti-virus non vengono aggiornati da molto tempo o che nel dispositivo è installata un'app bloccata. Un problema critico non può essere nascosto.

Controllo conformità

L'applicazione verifica automaticamente se il dispositivo è conforme ai requisiti di sicurezza aziendale. Le informazioni che indicano se il dispositivo soddisfa o meno i requisiti di sicurezza aziendale sono visualizzate nella sezione **Stato**.

- Il motivo per cui il dispositivo non è conforme ai requisiti di sicurezza aziendali (ad esempio, nel dispositivo sono state rilevate app bloccate).
- Il periodo di tempo entro il quale è necessario risolvere la mancata conformità (ad esempio, 24 ore).
- L'azione che verrà eseguita nel dispositivo se non si risolve la mancata conformità entro il periodo di tempo specificato (ad esempio il dispositivo verrà bloccato).
- L'azione eseguita per risolvere la mancata conformità con i requisiti di sicurezza aziendali.

Icona della barra di stato

Al termine della procedura guidata per il primo avvio, l'icona di Kaspersky Endpoint Security viene visualizzata nella barra di stato.

L'icona segnala il funzionamento dell'app e consente l'accesso alla finestra principale di Kaspersky Endpoint Security.

L'icona indica il funzionamento di Kaspersky Endpoint Security e segnala lo stato di protezione del dispositivo:

– Il dispositivo è protetto.

– Sono presenti problemi di protezione (ad esempio i database anti-virus non sono aggiornati oppure una nuova app installata non è stata esaminata).

Scansione del dispositivo

Anti-virus presenta diverse limitazioni:

- Quando Anti-Virus è in esecuzione, una minaccia rilevata nella memoria esterna del dispositivo (ad esempio una scheda SD) non può essere neutralizzata automaticamente nel profilo lavoro (Applicazioni con icona a forma di valigia, Configurazione del profilo lavoro Android). Kaspersky Endpoint Security for Android non ha accesso alla memoria esterna nel profilo lavoro. Le informazioni sugli oggetti rilevati vengono visualizzate nella sezione **Stato** dell'app. Per neutralizzare gli oggetti rilevati nella memoria esterna, i file dell'oggetto devono essere eliminati manualmente e la scansione del dispositivo deve essere riavviata.
- A causa di limitazioni tecniche, Kaspersky Endpoint Security for Android non può esaminare file con dimensioni pari o superiori a 2 GB. Durante una scansione, l'app ignora tali file senza inviare una notifica in merito.

Per avviare una scansione del dispositivo:

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare **Scansione**.

2. Selezionare l'ambito di scansione del dispositivo:

   - **Esegui scansione dell'intero dispositivo**. L'app esegue la scansione dell'intero file system del dispositivo.
   - **Esegui scansione delle app installate**. L'app esegue soltanto la scansione delle app installate.
   - **Scansione personalizzata**. L'app esegue la scansione della cartella selezionata o di un singolo file. È possibile selezionare un singolo oggetto (cartella o file) oppure una delle partizioni seguenti della memoria del dispositivo:
     - **Memoria dispositivo**. Memoria accessibile in lettura dell'intero dispositivo. È inclusa anche la partizione della memoria di sistema che contiene i file del sistema operativo.
     - **Memoria interna**. Partizione della memoria del dispositivo utilizzata per l'installazione delle app e l'archiviazione di contenuti multimediali, documenti e altri file.
     - **Memoria esterna**. Scheda di memoria SD esterna. Se non è installata una scheda SD esterna, questa opzione è nascosta.

L'accesso alle impostazioni di scansione virus potrebbe essere limitato dall'amministratore.

Per configurare la scansione virus:

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare → **Impostazioni** → **Anti-Virus** → **Scansione**.
2. Se si desidera che l'app rilevi adware e app utilizzabili dagli hacker per causare danni al dispositivo o ai dati quando viene eseguita una scansione, attivare l'interruttore **Adware, dialer e altro**.
3. Fare clic su **Azione se viene rilevata una minaccia**, quindi selezionare l'azione eseguita dall'app per impostazione predefinita:

   - **Quarantena**

     I file vengono memorizzati in Quarantena sotto forma di archivi, in modo che non possano danneggiare il dispositivo. Quarantena consente di eliminare o ripristinare i file che sono stati spostati in un archivio isolato.

   - **Richiedi azione**

     L'app richiede di selezionare un'azione per ogni oggetto rilevato: ignorare, mettere in quarantena o eliminare. Quando vengono rilevati più oggetti, è possibile applicare un'azione selezionata a tutti gli oggetti.

   - **Elimina**

     Gli oggetti rilevati verranno eliminati automaticamente. Non sono richieste azioni aggiuntive. Prima di eliminare un oggetto, Kaspersky Endpoint Security visualizzerà una notifica provvisoria sul rilevamento dell'oggetto.

   - **Ignora**

     Se gli oggetti rilevati sono stati ignorati, Kaspersky Endpoint Security avvisa in merito ai problemi di protezione del dispositivo. Le informazioni sugli oggetti ignorati vengono visualizzate nella sezione **Stato** dell'app. Per ogni minaccia ignorata, l'app propone azioni che è possibile eseguire per eliminare la minaccia. L'elenco degli oggetti ignorati può ad esempio cambiare se un file dannoso è stato eliminato o spostato. Per ricevere un elenco aggiornato delle minacce, eseguire una scansione completa del dispositivo. Per garantire la protezione ottimale dei dati, eliminare tutti gli oggetti rilevati.

Le informazioni sulle minacce rilevate e le azioni eseguite su di esse vengono registrate nei rapporti dell'app (→ **Rapporti**). È possibile scegliere di visualizzare i rapporti sulle operazioni di Anti-Virus.

Esecuzione di una scansione pianificata

Anti-virus presenta diverse limitazioni:

- Quando Anti-Virus è in esecuzione, una minaccia rilevata nella memoria esterna del dispositivo (ad esempio una scheda SD) non può essere neutralizzata automaticamente nel profilo lavoro (Applicazioni con icona a forma di valigia, Configurazione del profilo lavoro Android). Kaspersky Endpoint Security for Android non ha accesso alla memoria esterna nel profilo lavoro. Le informazioni sugli oggetti rilevati vengono visualizzate nella sezione **Stato** dell'app. Per neutralizzare gli oggetti rilevati nella memoria esterna, i file dell'oggetto devono essere eliminati manualmente e la scansione del dispositivo deve essere riavviata.
- A causa di limitazioni tecniche, Kaspersky Endpoint Security for Android non può esaminare file con dimensioni pari o superiori a 2 GB. Durante una scansione, l'app ignora tali file senza inviare una notifica in merito.

Per configurare la scansione completa per un dispositivo:

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare → **Impostazioni** → **Anti-Virus** → **Scansione**.
2. Toccare **Pianificazione**, quindi selezionare la frequenza di scansione completa:
   - **Settimanale**
   - **Giornaliera**
   - **Disabilitata**
   - **Dopo l'aggiornamento dei database**
3. Fare clic su **Giorno di inizio**, quindi selezionare il giorno della settimana in cui si desidera avviare la scansione completa.
4. Fare clic su **Ora di inizio**, quindi selezionare l'ora di avvio della scansione completa.

Verrà avviata una scansione completa del dispositivo in base alla pianificazione.

> In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

Modifica della modalità Protezione

Protezione in tempo reale consente di rilevare le minacce nei file aperti e di eseguire la scansione delle app durante l'installazione nel dispositivo in tempo reale. I database anti-virus e il servizio cloud Kaspersky Security Network (Protezione cloud) vengono utilizzati per garantire automaticamente la protezione.

Per modificare la modalità di protezione del dispositivo:

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare → **Impostazioni** → **Anti-Virus** → **Modalità di protezione in tempo reale**.

2. Selezionare la modalità Protezione del dispositivo:

   - **Disabilitata** La protezione è disabilitata.
   - **Consigliata**. Anti-virus esamina solo le app installate e i file della cartella Download. Anti-Virus esamina le nuove app al momento dell'installazione.
   - **Estesa**. Anti-Virus esamina tutti i file del dispositivo per verificare la presenza di eventuali oggetti dannosi quando su tali oggetti viene eseguita un'operazione (ad esempio quando vengono salvati, spostati o modificati). Anti-Virus esamina inoltre le nuove app al momento dell'installazione.

Le informazioni sulla modalità Protezione corrente sono visualizzate nella descrizione del componente.

L'accesso alle impostazioni di Protezione in tempo reale potrebbe essere limitato dall'amministratore.

Per abilitare Protezione cloud (KSN):

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare → **Impostazioni** → **Anti-Virus**.

2. Attivare l'interruttore **Protezione cloud (KSN)**.

   L'interruttore **Protezione cloud (KSN)** consente di gestire l'utilizzo di Kaspersky Security Network solo per la protezione in tempo reale di un dispositivo. Se la casella di controllo è deselezionata, Kaspersky Endpoint Security continua a utilizzare KSN per l'esecuzione di altri componenti dell'app.

   L'app ottiene quindi l'accesso alla Knowledge Base online di Kaspersky, con informazioni sulla reputazione di file e app. La scansione viene eseguita per le minacce per cui non sono state ancora aggiunte informazioni ai database anti-virus, ma che sono già disponibili in KSN. Il servizio cloud di Kaspersky Security Network garantisce l'esecuzione completa di Anti-virus e riduce la probabilità di falsi allarmi. Solo l'amministratore può disabilitare completamente l'uso di Kaspersky Security Network.

Per configurare Protezione in tempo reale:

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare → **Impostazioni** → **Anti-Virus** → **Modalità di protezione in tempo reale**.

2. Se si desidera che l'app rilevi adware e app utilizzabili dagli hacker per causare danni al dispositivo o ai dati quando viene eseguita una scansione, attivare l'interruttore **Adware, dialer e altro**.

3. Fare clic su **Azione se viene rilevata una minaccia**, quindi selezionare l'azione eseguita dall'app per impostazione predefinita:

   - **Quarantena**

     I file vengono memorizzati in Quarantena sotto forma di archivi, in modo che non possano danneggiare il dispositivo. Quarantena consente di eliminare o ripristinare i file che sono stati spostati in un archivio isolato.

   - **Elimina**

     Gli oggetti rilevati verranno eliminati automaticamente. Non sono richieste azioni aggiuntive. Prima di eliminare un oggetto, Kaspersky Endpoint Security visualizzerà una notifica provvisoria sul rilevamento dell'oggetto.

- **Ignora**

  Se gli oggetti rilevati sono stati ignorati, Kaspersky Endpoint Security avvisa in merito ai problemi di protezione del dispositivo. Le informazioni sugli oggetti ignorati vengono visualizzate nella sezione **Stato** dell'app. Per ogni minaccia ignorata, l'app propone azioni che è possibile eseguire per eliminare la minaccia. L'elenco degli oggetti ignorati può ad esempio cambiare se un file dannoso è stato eliminato o spostato. Per ricevere un elenco aggiornato delle minacce, eseguire una scansione completa del dispositivo. Per garantire la protezione ottimale dei dati, eliminare tutti gli oggetti rilevati.

Le informazioni sulle minacce rilevate e sulle azioni eseguite su di esse vengono registrate nei rapporti dell'app (→ **Impostazioni** → **Rapporti**). È possibile scegliere di visualizzare i rapporti sulle operazioni di Anti-Virus.

Aggiornamenti dei database anti-virus

Per aggiornare i database anti-virus dell'app:

Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare **Aggiornamento database**.

Aggiornamento dei database pianificato

L'app può aggiornare automaticamente i database anti-virus del dispositivo in base alla pianificazione specificata.

Per configurare la pianificazione degli aggiornamenti:

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare → **Impostazioni** → **Anti-Virus** → **Aggiornamento database**.
2. Fare clic su **Pianificazione** e selezionare la frequenza di aggiornamento:
   - **Settimanale**
   - **Giornaliera**
   - **Disabilitata**
3. Fare clic su **Giorno di inizio** e selezionare il giorno della settimana in cui si desidera eseguire l'aggiornamento.
4. Fare clic su **Ora di inizio** e selezionare l'ora di avvio dell'aggiornamento.

Gli aggiornamenti dei database anti-virus vengono avviati in base alla pianificazione.

In Android 12 o versioni successive l'app potrebbe eseguire questa attività successivamente al momento specificato se il dispositivo è in modalità Risparmio batteria.

Operazioni da eseguire in caso di furto o smarrimento del dispositivo

In caso di furto o smarrimento del dispositivo, contattare l'amministratore di sistema. L'amministratore può eseguire i comandi Antifurto nel dispositivo in remoto in base ai requisiti di sicurezza aziendale.

Se al dispositivo viene inviato un comando Reset Dispositivo, il controllo sul dispositivo andrà perso e i restanti comandi di Antifurto non funzioneranno.

Protezione Web

Per abilitare Protezione Web:

- Kaspersky Endpoint Security deve essere abilitato come servizio per le funzionalità di accessibilità.
- È necessario accettare l'Informativa relativa all'elaborazione dei dati a scopo di utilizzo di Protezione Web (Informativa di Protezione Web). Kaspersky Endpoint Security utilizza Kaspersky Security Network (KSN) per eseguire la scansione dei siti Web. L'Informativa di Protezione Web contiene i termini dello scambio di dati con KSN.

  L'amministratore può accettare l'Informativa di Protezione Web al posto dell'utente in Kaspersky Security Center. In questo caso non è necessario eseguire alcuna azione.

  Se l'amministratore non ha accettato l'Informativa di Protezione Web e ha inviato la richiesta all'utente, è necessario leggere e accettare l'Informativa di Protezione Web nelle impostazioni dell'app.

  Se l'amministratore non ha accettato l'Informativa di Protezione Web, Protezione Web non è disponibile.

Protezione Web nei dispositivi Android funziona solo nel browser Google Chrome (inclusa la funzionalità Schede personalizzate), in Huawei Browser e Samsung Internet Browser. Protezione Web per Samsung Internet Browser non blocca i siti su un dispositivo mobile se viene utilizzato un profilo lavoro e Protezione Web è abilitato solo per il profilo lavoro.

Per utilizzare sempre Protezione Web durante l'esplorazione del Web, impostare il Google Chrome o Samsung Internet Browser come browser predefinito.

Per impostare un browser supportato come browser predefinito e utilizzare sempre Protezione Web per la scansione dei siti Web:

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare → **Impostazioni** → **Protezione Web**.
2. Attivare l'interruttore **Protezione Web**.
3. Toccare **Imposta browser predefinito**.

   Questo pulsante viene visualizzato quando Protezione Web è abilitato e un browser supportato non è impostato come browser predefinito.

   Viene avviata la procedura guidata per la selezione del browser predefinito.
4. Seguire le istruzioni della procedura guidata.

La procedura guidata consente di impostare Google Chrome, Huawei Browser o Samsung Internet Browser come browser predefinito. Protezione Web esamina continuamente i siti Web durante l'esplorazione del Web.

Controllo app

Controllo app verifica che le app installate in un dispositivo mobile siano conformi ai requisiti di sicurezza aziendali. In Kaspersky Security Center l'amministratore crea elenchi di app consentite, bloccate, obbligatorie e consigliate in base ai requisiti di sicurezza aziendali. In seguito a Controllo app, Kaspersky Endpoint Security richiede di installare le app obbligatorie e consigliate e di rimuovere le app bloccate. È impossibile avviare le app bloccate nel dispositivo mobile.

Per installare le app obbligatorie e consigliate o rimuovere le app bloccate:

1. Accedere alla sezione **Stato** di Kaspersky Endpoint Security.
2. Selezionare le attività di Controllo app.
3. Eseguire le azioni consigliate.

Recupera certificato

Per ottenere un certificato per l'accesso alle risorse della rete aziendale:

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare → **Impostazioni** → **Avanzate** → **Recupera certificato**.
2. Specificare le credenziali dell'account di rete aziendale.
3. Se è stata ricevuta una password monouso dall'amministratore, selezionare la casella **Password monouso** e immettere la password ricevuta.

   Verrà avviata l'Installazione guidata certificato.
4. Seguire le istruzioni della procedura guidata.

Sincronizzazione con Kaspersky Security Center

La sincronizzazione del dispositivo mobile con il sistema di amministrazione remota Kaspersky Security Center è necessaria per la protezione e la configurazione del dispositivo secondo i requisiti di sicurezza aziendali. Il dispositivo viene automaticamente sincronizzato con Kaspersky Security Center, ma è possibile avviare la sincronizzazione anche manualmente. Dopo la prima sincronizzazione, il dispositivo viene aggiunto all'elenco dei dispositivi mobili gestiti tramite Kaspersky Security Center. L'amministratore può quindi configurare il dispositivo in base ai requisiti di sicurezza aziendali.

È possibile configurare le impostazioni di sincronizzazione durante l'esecuzione della procedura guidata di configurazione iniziale o nelle impostazioni di Kaspersky Endpoint Security. Le impostazioni di sincronizzazione devono essere configurate se Kaspersky Endpoint Security è stato installato utilizzando Google Play. Richiedere i valori delle impostazioni di sincronizzazione all'amministratore di sistema.

Modificare le impostazioni di sincronizzazione del dispositivo con il sistema di amministrazione remota Kaspersky Security Center solo quando richiesto dall'amministratore.

Per sincronizzare il dispositivo con Kaspersky Security Center:

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare → **Impostazioni** → **Sincronizzazione**.
2. Nella sezione **Impostazioni di sincronizzazione** specificare i valori delle seguenti impostazioni:
   - **Server**
   - **Porta**
   - **Gruppo**
   - **Indirizzo e-mail aziendale**

   Le impostazioni di sincronizzazione possono essere nascoste dall'amministratore.
3. Toccare **Sincronizza**.

Attivazione dell'app Kaspersky Endpoint Security for Android senza Kaspersky Security Center

Nella maggior parte dei casi, l'app Kaspersky Endpoint Security for Android installata nel dispositivo viene attivata dall'amministratore a livello centrale nel sistema di amministrazione remota Kaspersky Security Center. Se il dispositivo non è connesso a Kaspersky Security Center, è possibile immettere manualmente il codice di attivazione. Per ottenere il codice di attivazione, contattare l'amministratore.

Attivare l'app manualmente solo quando richiesto dall'amministratore.

Per immettere il codice di attivazione:

1. Nel messaggio di errore che informa che la licenza sta per scadere o è scaduta e che il dispositivo non è connesso ad Administration Server toccare **Attiva**.
2. Nella finestra di attivazione immettere il codice di attivazione fornito dall'amministratore, quindi toccare **Attiva**.
3. Se il codice di attivazione è corretto, viene visualizzata una notifica che informa dell'attivazione dell'app, oltre a indicare la data di scadenza della licenza.

L'app Kaspersky Endpoint Security for Android nel dispositivo è attivata.

Aggiornamento dell'app

Kaspersky Endpoint Security può essere aggiornato nei seguenti modi:

- Manualmente utilizzando Google Play. È possibile scaricare la nuova versione dell'app da Google Play e installarla nel dispositivo.
- Con l'aiuto dell'amministratore. L'amministratore può aggiornare in remoto la versione dell'app nel dispositivo utilizzando il sistema di amministrazione remota Kaspersky Security Center.

Aggiornamento dell'app da Google Play

L'amministratore può impedire di aggiornare l'app da Google Play.

L'app può essere aggiornata da Google Play seguendo la procedura di aggiornamento standard della piattaforma Android. Per l'aggiornamento dell'app devono essere soddisfatte le seguenti condizioni:

- È necessario disporre di un account Google.
- Il dispositivo deve essere associato all'account Google.
- Il dispositivo deve essere connesso a Internet.

Per ulteriori informazioni sulla creazione di un account Google, sull'associazione del dispositivo all'account o sull'utilizzo di Google Play Store, vedere il sito Web dell'assistenza di Google.

Aggiornamento dell'app tramite Kaspersky Security Center

L'aggiornamento dell'app tramite Kaspersky Security Center consiste nei passaggi seguenti:

1. L'amministratore invia al dispositivo mobile il pacchetto di distribuzione dell'app la cui versione soddisfa i requisiti di sicurezza aziendali.

   Viene visualizzata una richiesta di installazione di Kaspersky Endpoint Security nel dispositivo.

2. Accettare i termini e le condizioni dell'aggiornamento.

   La nuova versione dell'app verrà installata nel dispositivo. L'app non richiede ulteriori passaggi di configurazione dopo l'aggiornamento.

Rimozione dell'app

L'amministratore può impedire all'utente di rimuovere l'app autonomamente. In questo caso, non è possibile rimuovere Kaspersky Endpoint Security.

Kaspersky Endpoint Security può essere rimosso con i seguenti metodi:

- Manualmente nelle impostazioni dell'app.
- Manualmente nelle impostazioni del dispositivo.
- Con l'aiuto dell'amministratore. L'amministratore può rimuovere in remoto l'app dal dispositivo utilizzando il sistema di amministrazione remota Kaspersky Security Center.

Rimozione nelle impostazioni dell'app

Per rimuovere Kaspersky Endpoint Security dal dispositivo:

1. Nel riquadro di avvio veloce della finestra principale di Kaspersky Endpoint Security toccare → **Disinstalla app**.

   Verrà avviata la rimozione guidata dell'app.

2. Seguire le istruzioni della procedura guidata.

Rimozione nelle impostazioni del dispositivo

L'app viene rimossa seguendo la procedura standard per la piattaforma Android. Per rimuovere l'app, i diritti di amministratore per Kaspersky Endpoint Security devono essere disabilitati nelle impostazioni di sicurezza del dispositivo.

Nei dispositivi che eseguono Android 7.0 o versione successiva, se l'amministratore ha bloccato la rimozione, il dispositivo verrà bloccato se viene effettuato un tentativo di rimozione dell'app nelle impostazioni Android. Per sbloccare il dispositivo, contattare l'amministratore.

Rimozione tramite Kaspersky Security Center

La rimozione dell'app tramite Kaspersky Security Center consiste nei passaggi seguenti:

1. L'amministratore invia il comando di rimozione dell'app al dispositivo mobile.

   Il dispositivo mobile visualizza una richiesta di conferma della rimozione di Kaspersky Endpoint Security.

2. Confermare la rimozione dell'app.

   L'app verrà rimossa dal dispositivo.

App con icona a forma di valigia

Icona dell'applicazione nel profilo lavoro Android

Le app contrassegnate con un'icona a forma di valigetta (app aziendali) sono memorizzate nel dispositivo nel profilo lavoro Android (di seguito denominato anche "profilo lavoro"). Il *profilo lavoro Android* è un ambiente sicuro nel dispositivo in cui l'amministratore può gestire app e account senza limitare le possibilità di utilizzo dei dati personali da parte dell'utente.

Questo profilo consente di memorizzare i dati aziendali separatamente dai dati personali. In questo modo i dati aziendali rimangono riservati e protetti dal malware. Quando nel dispositivo viene creato un profilo lavoro, in quest'ultimo vengono automaticamente installate le seguenti app aziendali: Google Play Market, Google Chrome, Download, Kaspersky Endpoint Security for Android e così via.

App KNOX

L'app KNOX apre un contenitore KNOX nel dispositivo. Un *contenitore KNOX* è un ambiente sicuro nel dispositivo dell'utente con desktop, riquadro di avvio, app e widget specifici. L'amministratore può gestire app e account in un contenitore KNOX senza limitare le possibilità di utilizzo dei dati personali da parte dell'utente.

Un contenitore KNOX consente di memorizzare i dati aziendali separatamente dai dati personali. In questo modo i dati aziendali rimangono riservati e protetti dal malware.

In un contenitore KNOX è possibile accedere alla cassetta postale aziendale, alle informazioni di contatto dei dipendenti aziendali, all'archivio file e ad altre applicazioni.

Per maggiori informazioni sull'utilizzo di KNOX, visitare il *sito Web dell'assistenza tecnica di Samsung*.

Utilizzo dell'app Kaspersky Security for iOS

Questa sezione della Guida descrive le funzionalità e le operazioni disponibili per gli utenti dell'app Kaspersky Security for iOS.

Gli articoli in questa sezione comprendono tutte le opzioni potenzialmente disponibili o visibili in un dispositivo mobile. Il layout e il comportamento effettivi dell'app dipendono dal sistema di amministrazione remota implementato e dal modo in cui l'amministratore configura il dispositivo in base ai requisiti di sicurezza aziendali. Alcune funzioni e opzioni descritte in questa sezione potrebbero non essere applicabili all'effettiva esperienza dell'utente relativa all'app. In caso di domande sull'app nel dispositivo specifico, contattare l'amministratore.

Funzionalità dell'app

Kaspersky Security for iOS offre le seguenti funzionalità chiave.

Protezione dalle minacce online

Il componente Protezione Web garantisce la protezione dalle minacce online.

Protezione Web blocca i siti Web dannosi che distribuiscono codice dannoso e i siti Web di phishing progettati per rubare le informazioni riservate dell'utente e ottenere l'accesso ai conti personali. Protezione Web analizza i siti Web prima dell'apertura utilizzando il servizio cloud Kaspersky Security Network. Protezione Web controlla anche l'attività online delle app nel dispositivo dell'utente.

Per il corretto funzionamento di Protezione Web, è necessario consentire all'app di aggiungere una configurazione VPN.

Rilevamento jailbreak

Quando Kaspersky Security for iOS rileva un jailbreak, mostra un messaggio critico e informa l'amministratore del problema.

L'app non può garantire la sicurezza del dispositivo dell'utente, perché un jailbreak elude le funzionalità di sicurezza e può causare numerosi problemi, tra cui:

- Vulnerabilità della sicurezza
- Problemi di stabilità
- Interruzione dei servizi Apple
- Potenziali blocchi e arresti anomali
- Riduzione della durata della batteria
- Impossibilità di applicare gli aggiornamenti iOS

Installazione dell'app

Per installare l'app Kaspersky Security for iOS:

1. Trovare il messaggio e-mail con l'invito dell'amministratore a installare l'app Kaspersky Security for iOS dall'App Store.
2. Accedere all'App Store in uno dei seguenti modi:
   - Toccare il collegamento presente nel messaggio se si sta leggendo il messaggio nel dispositivo iOS in cui si desidera installare l'app.
   - Eseguire la scansione del codice QR utilizzando il dispositivo iOS nel quale si desidera installare l'app, se si sta leggendo il messaggio da un computer.

   Il collegamento di invito è valido per 24 ore. Se non si riesce a installare l'app per tempo, contattare l'amministratore per un nuovo invito.
3. Scaricare e installare l'app dall'App Store seguendo la procedura di installazione standard sulla piattaforma iOS.

L'app Kaspersky Security for iOS è installata nel dispositivo. Per proteggere il dispositivo, attivare l'app.

Attivazione dell'app

Per attivare l'app Kaspersky Security for iOS:

1. Avviare l'app nel proprio dispositivo.
2. Accettare i contratti e le informative selezionando le caselle di controllo del **Contratto di licenza con l'utente finale** e dell'**Informativa sulla Privacy per Prodotti e Servizi**.

   È inoltre possibile accettare l'**Informativa di Kaspersky Security Network** per consentire l'invio delle statistiche a Kaspersky Security Network. Questo migliora le prestazioni dell'app e ne garantisce il funzionamento senza interruzioni.
3. Toccare **Avanti**. L'app si connette al sistema di amministrazione remota di Kaspersky Security Center e ottiene le informazioni sulla licenza.
4. Consentire all'app di aggiungere una configurazione VPN. L'app utilizza la configurazione VPN per verificare la presenza di phishing nei siti Web e proteggere il dispositivo dal malware.
5. Consentire all'app di inviare notifiche push. L'app utilizza le notifiche per informare l'utente in merito ai problemi di sicurezza e allo stato della licenza.

L'app Kaspersky Security for iOS nel dispositivo è attivata.

Attivazione dell'app con un codice di attivazione

Quando si installa l'app Kaspersky Security for iOS nel dispositivo, l'app si connette al sistema di amministrazione remota di Kaspersky Security Center e ottiene automaticamente le informazioni sulla licenza. Se il dispositivo non è connesso a Kaspersky Security Center, è possibile immettere manualmente il codice di attivazione. Per ottenere il codice di attivazione, contattare l'amministratore.

Attivare l'app manualmente solo quando richiesto dall'amministratore.

Per immettere il codice di attivazione:

1. Nel messaggio che informa della mancata attivazione dell'app toccare **Attiva l'app**.
2. Nella finestra di attivazione immettere il codice di attivazione fornito dall'amministratore, quindi toccare **Attiva**.

   Se il codice di attivazione è corretto, viene visualizzata una notifica che informa dell'attivazione dell'app, oltre a indicare la data di scadenza della licenza.

L'app Kaspersky Security for iOS nel dispositivo è attivata.

Descrizione della finestra principale

L'aspetto della finestra principale varia leggermente a seconda della risoluzione dello schermo.

La finestra principale visualizza:

- Lo stato di protezione generale del dispositivo dell'utente.
- Messaggi che indicano lo stato dei componenti dell'app e i problemi di protezione.

Esistono tre tipi di messaggi:

- In verde. Messaggi relativi allo stato per informare che la protezione è attiva nell'area specificata.
- In giallo. Messaggi informativi per segnalare eventi che possono influire sulla sicurezza del dispositivo.
- In rosso. Messaggi critici per segnalare eventi di importanza critica per la sicurezza del dispositivo.

È possibile toccare un messaggio per visualizzare i dettagli.

Aggiornamento dell'app

È possibile scaricare la versione più recente dell'app Kaspersky Security for iOS dall'App Store e installarla nel dispositivo seguendo la procedura di aggiornamento standard sulla piattaforma iOS. È inoltre possibile attivare gli aggiornamenti automatici. L'app non richiede ulteriori passaggi di configurazione dopo l'aggiornamento.

Per l'aggiornamento dell'app devono essere soddisfatte le seguenti condizioni:

- È necessario disporre di un ID Apple.
- Il dispositivo deve essere associato all'ID Apple.
- Il dispositivo deve essere connesso a Internet.

Per ulteriori informazioni sulla creazione di un ID Apple, sull'associazione del dispositivo all'ID Apple o sull'utilizzo dell'App Store, visitare il sito Web del supporto Apple.

Rimozione dell'app

Per rimuovere l'app Kaspersky Security for iOS, seguire la procedura standard sulla piattaforma iOS:

1. Nella schermata iniziale tenere premuta l'icona dell'app.
2. Rimuovere l'app.

L'app Kaspersky Security for iOS viene rimossa dal dispositivo.

Licensing dell'applicazione

Questa sezione fornisce informazioni sulle condizioni generali relative alla gestione delle licenze di Kaspersky Security for Mobile.

Informazioni sul Contratto di licenza con l'utente finale

Il *Contratto di licenza con l'utente finale* è un accordo vincolante tra l'utente e AO Kaspersky Lab, in cui sono definiti i termini e le condizioni di utilizzo di Kaspersky Security for Mobile.

Leggere attentamente i termini e le condizioni del Contratto di licenza con l'utente finale prima di utilizzare Kaspersky Security for Mobile.

È possibile visualizzare i termini e le condizioni del Contratto di licenza con l'utente finale nei seguenti modi:

- Durante l'installazione dei componenti di Kaspersky Security for Mobile.
- Leggendo il file license.txt incluso nell'archivio autoestraente del kit di distribuzione per l'installazione dell'app Kaspersky Endpoint Security for Android.
- Nella sezione **Informazioni sull'app** di Kaspersky Endpoint Security for Android.
- Nella sezione **Informazioni sull'app** → **Contratti e informative** in Kaspersky Security for iOS.
- Nella sezione **Avanzate** → **Contratti di licenza accettati** nelle proprietà di Administration Server. Questa funzionalità è disponibile in Kaspersky Security Center versione 12.1 e successiva.

Accettando il Contratto di licenza con l'utente finale durante l'installazione dei componenti di Kaspersky Security for Mobile, si accettano i termini e le condizioni del Contratto di licenza con l'utente finale. Se non si accettano i termini del Contratto di licenza con l'utente finale, è necessario annullare l'installazione dei componenti di Kaspersky Security for Mobile e non utilizzarli.

Informazioni sulla licenza

Una licenza è un diritto limitato di utilizzare la soluzione integrata Kaspersky Security for Mobile fornita alle condizioni del Contratto di licenza con l'utente finale.

Una licenza corrente consente di usufruire dei seguenti tipi di servizi:

- Utilizzare le app nei dispositivi mobili in conformità alle condizioni del Contratto di licenza con l'utente finale.
- Ricevere assistenza tecnica.

L'ambito dei servizi disponibili e le condizioni per l'utilizzo dell'app dipendono dal tipo di licenza utilizzata per attivare l'app.

Sono disponibili i seguenti tipi di licenza:

- *Di prova*.

  Una licenza gratuita che consente di valutare Kaspersky Security for Mobile.

La licenza di prova ha una validità di 30 giorni. Allo scadere della licenza di prova, l'app mobile Kaspersky Endpoint Security for Android e l'app mobile Kaspersky Security for iOS arrestano l'esecuzione della maggior parte delle funzioni tranne la sincronizzazione con Administration Server. Per continuare a utilizzare l'app, è necessario acquistare una licenza commerciale.

- *Commerciale*.

  Una licenza fornita al momento dell'acquisto di Kaspersky Security for Mobile.

  Allo scadere della licenza commerciale, l'app mobile continua a funzionare, ma con funzionalità limitate.

  Nella modalità con funzionalità limitate i seguenti componenti sono disponibili a seconda dell'app.

  - App Kaspersky Endpoint Security for Android:
    - **Anti-Virus**. Protezione in tempo reale e Scansione virus del dispositivo sono disponibili, mentre gli aggiornamenti dei database anti-virus non sono disponibili.
    - **Antifurto**. È disponibile solo l'invio di comandi al dispositivo mobile.
    - **Sincronizzazione con Administration Server**.

    Kaspersky Endpoint Security for Android interrompe lo scambio di informazioni con Kaspersky Security Network, Google Analytics per Firebase, Attestazione SafetyNet, Firebase Performance Monitoring e Crashlytics se la chiave di Kaspersky è bloccata, se la licenza di prova scade o in caso di licenza mancante (il codice di attivazione viene rimosso dal criterio di gruppo).

  - App Kaspersky Security for iOS:
    - **Sincronizzazione con Administration Server**.

    Kaspersky Security for iOS interrompe lo scambio di informazioni con Kaspersky Security Network se la licenza di prova scade o se manca una licenza (il codice di attivazione viene rimosso dal criterio di gruppo).

  I componenti rimanenti dell'app mobile non sono disponibili per l'utente del dispositivo. L'amministratore può utilizzare i criteri di gruppo per gestire questi componenti in modalità con funzionalità limitate. Non è possibile utilizzare i criteri di gruppo per configurare gli altri componenti dell'app.

  Per continuare a utilizzare l'app con funzionalità complete, è necessario rinnovare la licenza commerciale. È consigliabile rinnovare il periodo di validità della licenza o acquistarne una nuova prima della scadenza della licenza corrente per garantire la massima protezione del computer da tutte le minacce alla sicurezza.

Informazioni sull'abbonamento

L'abbonamento per Kaspersky Security for Mobile consente di utilizzare l'app mobile con i parametri selezionati (data di scadenza dell'abbonamento, numero di dispositivi mobili protetti). È possibile ordinare l'abbonamento per Kaspersky Security for Mobile dal fornitore del servizio (ad esempio il proprio provider di servizi Internet). L'abbonamento può essere rinnovato manualmente o automaticamente oppure è possibile annullare l'abbonamento. È possibile gestire l'abbonamento nel sito Web del fornitore del servizio.

L'abbonamento può essere limitato (ad esempio annuale) o illimitato (senza data di scadenza). Per continuare a utilizzare Kaspersky Security for Mobile dopo la scadenza del periodo di validità di un abbonamento limitato, è necessario rinnovare l'abbonamento. L'abbonamento illimitato viene rinnovato automaticamente se il pagamento anticipato al fornitore del servizio è stato eseguito per tempo.

Se l'abbonamento è limitato, al momento della scadenza può essere offerto un periodo di tolleranza per il rinnovo dell'abbonamento, durante il quale le app manterranno le proprie funzionalità. La disponibilità e la durata di tale periodo di tolleranza sono a discrezione del fornitore del servizio.

Per utilizzare Kaspersky Security for Mobile con un abbonamento, è necessario applicare il codice di attivazione ricevuto dal fornitore del servizio. In seguito all'applicazione del codice di attivazione, viene installata la chiave per la licenza che consente di utilizzare l'applicazione con abbonamento.

Le opzioni possibili per la gestione dell'abbonamento possono variare a seconda del fornitore del servizio. Il fornitore del servizio potrebbe non offrire un periodo di tolleranza per il rinnovo dell'abbonamento durante il quale le app manterranno le proprie funzionalità.

I codici di attivazione acquistati con l'abbonamento non possono essere utilizzati per attivare le versioni precedenti di Kaspersky Security for Mobile.

Informazioni sulla chiave

Una *chiave* è una sequenza di bit applicabile per attivare e quindi utilizzare la soluzione integrata Kaspersky Security for Mobile in conformità alle condizioni del Contratto di licenza con l'utente finale. Le chiavi sono generate dagli specialisti di Kaspersky.

È possibile aggiungere una chiave per l'app mobile utilizzando un file chiave o un codice di attivazione:

- Se l'organizzazione ha distribuito la suite di software Kaspersky Security Center, è necessario applicare il file chiave e distribuirlo alle app mobili Android. La chiave viene visualizzata nell'interfaccia di Kaspersky Security Center e nell'interfaccia dell'app mobile Android sotto forma di sequenza alfanumerica univoca.

  In seguito all'aggiunta delle chiavi, è possibile sostituirle con altre chiavi.

  Non è possibile attivare l'app Kaspersky Security for iOS con un file chiave.

- Se l'azienda non utilizza Kaspersky Security Center, è necessario condividere il codice di attivazione con l'utente. L'utente immette tale codice di attivazione nell'app mobile iOS o Android. La chiave viene visualizzata nell'interfaccia dell'app mobile come sequenza alfanumerica univoca.

La chiave può essere bloccata da Kaspersky se, ad esempio, vengono violate le condizioni del Contratto di licenza con l'utente finale. Se la chiave è bloccata, l'app mobile arresta l'esecuzione di tutte le funzioni tranne la sincronizzazione con Administration Server. Per continuare a utilizzare l'app, è necessario aggiungere una chiave diversa.

Informazioni sul codice di attivazione

Il codice di attivazione è una sequenza univoca di 20 caratteri alfanumerici. Si immette un codice di attivazione per aggiungere una chiave che attiva l'app mobile Kaspersky Endpoint Security for Android o l'app mobile Kaspersky Security for iOS. Il codice di attivazione viene ricevuto all'indirizzo e-mail specificato in seguito all'acquisto della soluzione integrata Kaspersky Security for Mobile o all'ordine della versione di prova di Kaspersky Security for Mobile.

Per attivare l'app mobile con un codice di attivazione, è necessario l'accesso a Internet per connettersi ai server di attivazione Kaspersky.

Se il codice di attivazione è stato smarrito in seguito all'attivazione dell'app, è possibile ripristinarlo. Può essere necessario il codice di attivazione, ad esempio per registrarsi a Kaspersky CompanyAccount. Per ripristinare il codice di attivazione, contattare l'Assistenza tecnica di Kaspersky.

Informazioni sul file chiave

Un *file chiave* è un file con estensione .key ricevuto da Kaspersky. Lo scopo di un file chiave è quello di aggiungere una chiave per l'attivazione dell'app Kaspersky Endpoint Security for Android.

Non è possibile attivare l'app Kaspersky Security for iOS con un file chiave.

Il file chiave viene ricevuto all'indirizzo e-mail specificato in seguito all'acquisto della soluzione integrata Kaspersky Security for Mobile o all'ordine della versione di prova di Kaspersky Security for Mobile.

Non è necessario connettersi ai server di attivazione di Kaspersky per attivare l'applicazione con un file chiave.

È possibile ripristinare un file chiave eliminato accidentalmente. Potrebbe essere necessario un file chiave per registrare ad esempio un Kaspersky CompanyAccount.

Per ripristinare un file chiave, eseguire una delle seguenti operazioni:

- Contattare il venditore della licenza.
- Ricevere un file chiave attraverso il sito Web di Kaspersky utilizzando il codice di attivazione disponibile.

Trasmissione dei dati in Kaspersky Endpoint Security for Android

Kaspersky Security for Mobile è conforme al Regolamento generale sulla protezione dei dati.

Per installare l'app, il soggetto o un utente del dispositivo deve leggere e accettare i termini del Contratto di licenza con l'utente finale. È inoltre possibile configurare un criterio per accettare le informative elencate di seguito a livello globale per tutti gli utenti. In caso contrario, agli utenti verrà richiesto tramite una notifica nella schermata principale dell'app di accettare le seguenti informative relative all'elaborazione dei dati personali dell'utente:

- Informativa di Kaspersky Security Network
- Informativa relativa all'elaborazione dei dati per Protezione Web
- Informativa relativa all'elaborazione dei dati per finalità di marketing

Se si sceglie di accettare le informative a livello globale, le versioni delle informative accettate tramite Kaspersky Security Center devono corrispondere alle versioni già accettate dagli utenti. In caso contrario, gli utenti verranno informati del problema e verrà loro richiesto di accettare la versione di un'informativa corrispondente alla versione accettata a livello globale dall'amministratore. Anche lo stato del dispositivo nel plug-in di Kaspersky Security for Mobile (Devices) diventerà *Avviso*.

L'utente può accettare i termini di un'informativa o rifiutarli in qualsiasi momento nella sezione **Informazioni sull'app** nelle impostazioni di Kaspersky Endpoint Security for Android.

Scambio di informazioni con Kaspersky Security Network

Per migliorare la protezione in tempo reale, Kaspersky Endpoint Security for Android utilizza il servizio cloud Kaspersky Security Network per l'esecuzione dei seguenti componenti:

- **Anti-Virus.** L'app ottiene accesso alla Knowledge Base online di Kaspersky, con informazioni sulla reputazione di file e app. La scansione viene eseguita per le minacce per cui non sono state ancora aggiunte informazioni ai database anti-virus, ma che sono già disponibili in KSN. Il servizio cloud di Kaspersky Security Network garantisce l'esecuzione completa di Anti-virus e riduce la probabilità di falsi allarmi.

- **Protezione Web.** L'app utilizza i dati ricevuti da KSN per esaminare i siti Web prima dell'apertura. L'app determina inoltre la categoria del sito Web per controllare l'accesso a Internet degli utenti in base agli elenchi delle categorie consentite e bloccate (ad esempio, la categoria "Comunicazioni di rete").

- **Controllo app.** L'app determina la categoria dell'app per limitare l'avvio delle app che non soddisfano i requisiti di sicurezza aziendali in base agli elenchi delle categorie consentite e bloccate (ad esempio, la categoria "Giochi").

Le informazioni sul tipo di dati inviati a Kaspersky durante l'utilizzo di KSN con Anti-Virus e Controllo app sono disponibili nel Contratto di licenza con l'utente finale. Accettando i termini e le condizioni del Contratto di licenza, si accetta il trasferimento di queste informazioni.

Le informazioni sul tipo di dati inviati a Kaspersky durante l'utilizzo di KSN con Protezione Web sono disponibili nell'Informativa relativa all'elaborazione dei dati per Protezione Web. Accettando i termini e le condizioni dell'Informativa, si accetta il trasferimento di queste informazioni.

Le informazioni sul tipo di dati statistici inviati a Kaspersky durante l'utilizzo di KSN con l'app mobile Kaspersky Endpoint Security for Android sono disponibili nell'Informativa di Kaspersky Security Network. Accettando i termini e le condizioni dell'Informativa, si accetta il trasferimento di queste informazioni.

Trasmissione dei dati nell'ambito del Contratto di licenza con l'utente finale

Se il Codice di attivazione viene usato per attivare il Software, al fine di verificare l'uso legittimo del Software, l'Utente finale accetta di fornire periodicamente al Titolare dei diritti le seguenti informazioni:

- formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; indirizzo IPv4 del servizio Web a cui è stato eseguito l'accesso; dimensioni del contenuto della richiesta all'infrastruttura del Titolare dei diritti; ID protocollo; codice di attivazione del software; tipo di compressione dei dati; ID software; set di ID del Software che può essere attivato nel dispositivo dell'utente; localizzazione del software; versione completa del software; ID dispositivo univoco; data e ora nel dispositivo dell'utente; ID installazione Software (PCID); versione del sistema operativo, numero build del sistema operativo, numero di aggiornamento del sistema operativo, edizione del sistema operativo, informazioni estese sull'edizione del sistema operativo; modello dispositivo; famiglia del sistema operativo; formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; tipo di checksum per l'oggetto elaborato; intestazione licenza Software; ID di un centro di attivazione regionale; data e ora di creazione della chiave di licenza Software; ID della licenza Software; ID del modello di informazioni utilizzato per fornire la licenza Software; data e ora di scadenza della licenza Software; stato corrente della chiave di licenza Software; tipo di licenza Software utilizzata; tipo di licenza utilizzata per attivare il Software; ID software derivato dalla licenza;

Per proteggere il computer da minacce al sistema informatico, l'Utente finale accetta di fornire periodicamente al Titolare dei diritti le seguenti informazioni:

- tipo di checksum per l'oggetto elaborato; checksum dell'oggetto elaborato; ID componente Software;

- ID del record attivato nei database anti-virus del Software; timestamp del record attivato nei database anti-virus del Software; tipo di record attivato nei database anti-virus del Software; nome del malware rilevato o del software legittimo che può essere utilizzato per danneggiare i dati o il dispositivo dell'utente;

- nome del punto vendita da cui è stata installata l'applicazione; nome pacchetto applicazioni; chiave pubblica utilizzata per firmare il file APK; checksum del certificato utilizzato per firmare il file APK; timestamp del certificato digitale;

- versione completa del software; ID aggiornamento software; tipo di software installato; identificatore configurazione; risultato dell'azione del Software; codice errore;

- numeri che derivano dal file APK dell'applicazione Android secondo determinate regole matematiche e che non consentono il ripristino del contenuto del file originale; questi dati non contengono nomi di file, percorsi di file, indirizzi, numeri di telefono o altre informazioni personali degli utenti.

Se l'Utente utilizza i server degli aggiornamenti del Titolare dei diritti per scaricare gli Aggiornamenti, al fine di migliorare l'efficienza della procedura di aggiornamento, l'Utente finale accetta di fornire periodicamente al Titolare dei diritti le seguenti informazioni:

- ID software derivato dalla licenza; versione completa del software; ID della licenza Software; tipo di licenza Software utilizzata; ID installazione Software (PCID); ID di avvio aggiornamento del Software; indirizzo Web in fase di elaborazione.

Il Titolare dei diritti può utilizzare tali informazioni anche per ricevere informazioni statistiche sulla distribuzione e l'utilizzo del software.

Le informazioni ricevute sono protette da Kaspersky in conformità ai requisiti previsti dalla legge. Le informazioni originali ricevute vengono archiviate in formato criptato e vengono distrutte man mano che vengono accumulate (due volte all'anno) o su richiesta dell'Utente. Le statistiche generali sono archiviate a tempo indeterminato.

Trasmissione dei dati nell'ambito dell'Informativa di Kaspersky Security Network

L'uso di KSN potrebbe determinare un incremento dell'efficacia della protezione fornita dal Software nei confronti delle minacce alla sicurezza delle informazioni e della rete.

Se si utilizza una licenza per 5 o più nodi, il Titolare dei diritti riceverà ed elaborerà automaticamente i seguenti dati durante l'utilizzo di KSN:

- ID del record attivato nei database anti-virus del Software; timestamp del record attivato nei database anti-virus del Software; tipo di record attivato nei database anti-virus del Software; data e ora di rilascio dei database del Software; versione del sistema operativo, numero build del sistema operativo, numero di aggiornamento del sistema operativo, edizione del sistema operativo, informazioni estese sull'edizione del sistema operativo; versione Service Pack del sistema operativo; caratteristiche di rilevamento; checksum (MD5) dell'oggetto elaborato; nome dell'oggetto elaborato; contrassegno indicante se l'oggetto elaborato è un file PE; checksum (MD5) della maschera che ha bloccato il servizio Web; checksum (SHA256) dell'oggetto elaborato; dimensioni dell'oggetto elaborato; codice del tipo di oggetto; decisione del Software sull'oggetto elaborato; percorso dell'oggetto elaborato; codice directory; versione del componente del Software; versione delle statistiche inviate; indirizzo del servizio Web al quale è stato eseguito l'accesso (URL, IP); tipo di client utilizzato per accedere al servizio Web; indirizzo IPv4 del servizio Web a cui è stato eseguito l'accesso; indirizzo IPv6 del servizio Web a cui è stato eseguito l'accesso; indirizzo Web dell'origine della richiesta del servizio Web (provenienza); indirizzo Web in fase di elaborazione;

- informazioni sugli oggetti analizzati (versione applicazione da AndroidManifest.xml; decisione del Software sull'applicazione; metodo utilizzato per ottenere la decisione del Software sull'applicazione; nome pacchetto del programma di installazione del punto vendita; nome pacchetto (o nome bundle) da AndroidManifest.xml; categoria Google SafetyNet; contrassegno indicante se SafetyNet è abilitato nel dispositivo; valore SHA256 della risposta Google SafetyNet; scherma firme APK per il certificato APK; codice versione del Software

installato; numero di serie del certificato utilizzato per firmare il file APK; nome del file APK file installato; percorso del file APK installato; emittente del certificato utilizzato per firmare il file APK; chiave pubblica utilizzata per firmare il file APK; checksum del certificato utilizzato per firmare il file APK; data e ora di scadenza del certificato; data e ora di emissione del certificato; versione delle statistiche inviate; algoritmo per il calcolo dell'impronta digitale del certificato digitale; hash MD5 del file APK installato; hash MD5 del file DEX posizionato all'interno del file APK; autorizzazioni concesse dinamicamente all'applicazione; versione software di terze parti; contrassegno indicante se l'applicazione è il programma di messaggistica SMS predefinito; contrassegno indicante se l'applicazione dispone dei diritti di amministratore del dispositivo; contrassegno indicante se l'applicazione è presente nel catalogo di sistema; contrassegno indicante se l'applicazione utilizza servizi di accessibilità);

- informazioni su tutte le azioni e gli oggetti potenzialmente dannosi (contenuti frammentati dell'oggetto elaborato; data e ora di scadenza del certificato; data e ora di emissione del certificato; ID della chiave appartenente al keystore utilizzato per il criptaggio; protocollo utilizzato per scambiare i dati con KSN; ordine frammento nell'oggetto elaborato; dati del log interno, generato dal modulo del Software anti-virus per un oggetto elaborato; nome dell'autorità di emissione del certificato; chiave pubblica del certificato; algoritmo di calcolo della chiave pubblica del certificato; numero di serie del certificato; data e ora della firma dell'oggetto; nome del proprietario del certificato e impostazioni; identificazione personale del certificato digitale dell'oggetto esaminato e algoritmo hash; data e ora dell'ultima modifica dell'oggetto elaborato; data e ora di creazione di un oggetto elaborato; oggetti o relativi componenti elaborati; descrizione di un oggetto elaborato come definito nelle proprietà dell'oggetto; formato dell'oggetto elaborato; tipo di checksum per l'oggetto elaborato; checksum (MD5) dell'oggetto elaborato; nome dell'oggetto elaborato; checksum (SHA256) dell'oggetto elaborato; dimensioni dell'oggetto elaborato; nome del fornitore del software; decisione del Software sull'oggetto elaborato; versione dell'oggetto elaborato; origine della decisione presa per l'oggetto elaborato; checksum dell'oggetto elaborato; nome applicazione padre; percorso dell'oggetto elaborato; informazioni sui risultati del controllo firme del file; chiave della sessione di accesso; algoritmo di criptaggio per la chiave della sessione di accesso; ora di archiviazione per l'oggetto elaborato; algoritmo per il calcolo dell'impronta digitale del certificato digitale);

- tipo build, ad esempio "user" o "eng"; nome completo del prodotto; prodotto/produttore hardware; se è possibile installare le app esternamente a Google Play; stato del servizio cloud per la verifica di app Google; stato del servizio cloud per la verifica di app Google installate tramite ADB; nome codice di sviluppo corrente o "REL" per build di produzione; numero build incrementale; stringa versione visibile all'utente; nome del dispositivo dell'utente; ID build del Software visibile all'utente; impronta digitale firmware; ID firmware; contrassegno indicante se il dispositivo è collegato a un rooter; sistema operativo; nome del software; tipo di licenza Software utilizzata;

- informazioni sulla qualità dei servizi KSN (protocollo utilizzato per lo scambio dati con KSN; ID del servizio KSN a cui ha avuto accesso il Software; data e ora di interruzione della ricezione di statistiche; numero di connessioni KSN provenienti dalla cache; numero di richieste per le quali è stata trovata una risposta nel database delle richieste locale; numero di connessioni KSN non riuscite; numero di transazioni KSN non riuscite; distribuzione temporanea delle richieste a KSN annullate; distribuzione temporanea delle connessioni KSN non riuscite; distribuzione temporanea delle transazioni KSN non riuscite; distribuzione temporanea delle connessioni KSN riuscite; distribuzione temporanea delle transazioni KSN riuscite; distribuzione temporanea delle richieste a KSN riuscite; distribuzione temporanea delle richieste a KSN in timeout; numero di nuove connessioni KSN; numero di richieste a KSN non riuscite a causa di errori di routing; numero di richieste non riuscite a causa della disattivazione di KSN nelle impostazioni del Software; numero di richieste a KSN non riuscite a causa di problemi di rete; numero di connessioni KSN riuscite; numero di transazioni KSN riuscite; numero totale di richieste KSN; data e ora di inizio ricezione delle statistiche;

- ID dispositivo; versione completa del software; ID aggiornamento software; ID installazione Software (PCID); tipo di software installato;

- altezza dello schermo del dispositivo; larghezza dello schermo del dispositivo; informazioni sull'applicazione sovrapposta: hash MD5 del file APK; informazioni sull'applicazione sovrapposta: hash MD5 del file classes.dex; informazioni sull'applicazione sovrapposta: nome del file APK; informazioni sull'applicazione sovrapposta: percorso del file APK senza il nome file; altezza sovrapposizione; informazioni sul Software sovrapposto: hash MD5 del file APK; informazioni sull'applicazione sovrapposta: hash MD5 del file classes.dex; informazioni sull'applicazione sovrapposta: nome file APK; informazioni sull'applicazione sovrapposta: percorso del file APK

senza il nome file; informazioni sull'applicazione sovrapposta: nome del pacchetto dell'applicazione (per l'applicazione sovrapposta: se l'annuncio viene visualizzato su un desktop vuoto, il valore deve essere "launcher"); data e ora della sovrapposizione; informazioni sull'applicazione sovrapposta: nome pacchetto applicazioni; larghezza sovrapposizione;

- impostazioni del punto di accesso Wi-Fi in uso (tipo di dispositivo rilevato, impostazioni DHCP (checksum dell'IPv6 locale del gateway, IPv6 DHCP, IPv6 DNS1, IPv6 DNS2); checksum della lunghezza del prefisso di rete; checksum dell'indirizzo locale (IPv6); impostazioni DHCP (checksum dell'indirizzo IP locale del gateway, IP DHCP, IP DNS1, IP DNS2 e subnet mask); contrassegno indicante se il dominio DNS esiste; checksum dell'indirizzo IPv6 locale assegnato; checksum dell'indirizzo IPv4 locale assegnato; contrassegno indicante se il dispositivo è collegato; tipo di autenticazione della rete Wi-Fi; elenco delle reti Wi-Fi disponibili e relative impostazioni; checksum (MD5 con salting) dell'indirizzo MAC del punto di accesso; checksum (SHA256 con salting) dell'indirizzo MAC del punto di accesso; tipi di connessione supportati dal punto di accesso Wi-Fi; tipo di criptaggio della rete Wi-Fi; ora locale di inizio e fine della connessione alla rete Wi-Fi; ID rete Wi-Fi in base all'indirizzo MAC del punto di accesso; ID rete Wi-Fi in base al nome della rete Wi-Fi; ID rete Wi-Fi in base al nome della rete Wi-Fi e all'indirizzo MAC del punto di accesso; potenza del segnale Wi-Fi; nome della rete Wi-Fi; set di protocolli di autenticazione supportato da questa configurazione; protocollo di autenticazione utilizzato per una connessione WPA-EAP; protocollo di autenticazione interna; set di protocolli di crittografie di gruppo supportato da questa configurazione; set di protocolli di gestione delle chiavi supportato da questa configurazione; categoria di privacy finale della rete nel Software; categoria di sicurezza finale della rete nel Software; set di crittografia a blocchi per WPA supportato da questa configurazione; set di protocolli di sicurezza supportato da questa configurazione;

- data e ora di installazione del Software; data di attivazione del software; identificatore dell'organizzazione partner tramite cui è stato inserito l'ordine di licenza Software; ID software derivato dalla licenza; numero di serie della chiave di licenza Software; localizzazione del software; contrassegno indicante se è abilitata la partecipazione a KSN; ID del software concesso in licenza; ID della licenza Software; ID sistema operativo; versione del sistema operativo.

Inoltre, per poter conseguire l'obiettivo di aumentare l'efficacia della protezione fornita dal Software, il Titolare dei diritti può ricevere degli oggetti che potrebbero essere utilizzati da intrusi per danneggiare il computer e creare minacce alla sicurezza delle informazioni.

L'inserimento delle informazioni sopra indicate nel sistema KSN è facoltativo. È possibile scegliere di interrompere la partecipazione a Kaspersky Security Network in qualsiasi momento.

Trasmissione dei dati nell'ambito dell'Informativa relativa all'elaborazione dei dati per Protezione Web

Secondo l'Informativa di Protezione Web il Titolare dei diritti elabora i dati per la funzionalità Protezione Web. Lo scopo dichiarato include il rilevamento delle minacce Web e la definizione delle categorie dei siti Web visitati utilizzando il servizio cloud Kaspersky Security Network (KSN).

Con il consenso dell'Utente, i seguenti dati verranno inviati automaticamente e regolarmente al Titolare dei diritti nell'ambito dell'Informativa di Protezione Web:

- Versione del prodotto; Identificatore univoco del dispositivo; ID installazione; Tipo di prodotto.

- URL della pagina, numero di porta, protocollo URL, URL, con riferimento alle informazioni richieste.

Trasmissione dei dati nell'ambito dell'Informativa relativa all'elaborazione dei dati per finalità di marketing

Il Titolare dei diritti utilizza sistemi informatici di terze parti per elaborare i dati. Le modalità di trattamento dei dati di tali sistemi sono disciplinate dalle rispettive dichiarazioni sulla privacy. Di seguito sono elencati i servizi di cui si avvale il Titolare dei diritti e i dati da essi elaborati:

Google Analytics per Firebase

Durante l'utilizzo del Software, i seguenti dati verranno trasmessi automaticamente e regolarmente a Google Analytics per Firebase per lo scopo dichiarato:

- Informazioni sull'app (versione e ID dell'app, ID dell'app nel servizio Firebase, ID istanza nel servizio Firebase, nome dello store da cui è stata scaricata l'applicazione, data e ora del primo avvio del Software)
- ID di installazione dell'app nel dispositivo e metodo di installazione nel dispositivo
- Informazioni sull'area geografica e sulla lingua
- Informazioni sulla risoluzione dello schermo del dispositivo
- Informazioni sull'utente che ha ottenuto la root
- Informazioni di diagnostica sul dispositivo dal servizio SafetyNet Attestation
- Informazioni sull'impostazione di Kaspersky Endpoint Security for Android come funzione di accessibilità.
- Informazioni sulle transizioni fra schermate dell'applicazione, durata delle sessioni, inizio e fine di una sessione della schermata, nome della schermata
- Informazioni sul protocollo utilizzato per inviare i dati al servizio Firebase, la versione e l'ID del metodo di invio utilizzato
- Dettagli sul tipo e i parametri dell'evento per cui vengono inviati i dati
- Informazioni sulla licenza dell'app, la disponibilità e il numero di dispositivi
- Informazioni sulla frequenza degli aggiornamenti del database anti-virus e sulla sincronizzazione con Administration Server
- Informazioni sulla console di amministrazione (Kaspersky Security Center o sistemi EMM di terze parti)
- ID Android
- ID inserzionista
- informazioni sull'Utente: fascia d'età e sesso, identificativo del paese di residenza ed elenco di interessi
- informazioni sul computer dell'Utente in cui è installato il Software: nome del produttore del computer, tipo di computer, modello, versione e lingua (impostazioni locali) del sistema operativo, informazioni sull'applicazione aperta per la prima volta negli ultimi 7 giorni e sull'applicazione aperta per la prima volta più di 7 giorni fa

  I dati vengono trasmessi a FireBase tramite un canale protetto. Le informazioni sul trattamento dei dati da parte di Firebase sono disponibili su: https://firebase.google.com/support/privacy.

Attestazione SafetyNet

Durante l'utilizzo del Software, i seguenti dati verranno trasmessi automaticamente e regolarmente all'attestazione SafetyNet per lo scopo dichiarato:

- ora del controllo dispositivo

- informazioni sul software, nome e data dei certificati software
- risultati del controllo dispositivo
- controlli casuali dell'ID per verificare il risultati del dispositivo di controllo

  I dati vengono inoltrati all'attestazione SafetyNet tramite un canale protetto. Le informazioni sul trattamento dei dati da parte di SafetyNet Attestation sono disponibili su: https://policies.google.com/privacy.

Monitoraggio delle prestazioni di Firebase

Durante l'utilizzo del Software, i seguenti dati verranno trasmessi automaticamente e regolarmente a Firebase Performance Monitoring per lo scopo dichiarato:

- ID di installazione univoco
- nome pacchetto applicazioni
- versione del software installato
- livello della batteria e stato di carica della batteria
- operatore
- stato dell'app in primo piano o in background
- geografia
- Indirizzo IP
- codice lingua dispositivo
- informazioni sulla connessione di rete/via radio
- ID istanza Software pseudonimo
- RAM e dimensioni del disco
- contrassegno indicante se il dispositivo è collegato a un rooter o se è stato manomesso con jailbreak
- potenza del segnale
- durata delle tracce automatiche
- rete e le seguenti informazioni corrispondenti: codice di risposta, dimensioni payload in byte, tempo di risposta
- descrizione del dispositivo

  I dati vengono trasmessi a Firebase Performance Monitoring tramite un canale protetto. Le informazioni sul trattamento dei dati da parte di Firebase Performance Monitoring sono disponibili all'indirizzo: https://firebase.google.com/support/privacy.

Crashlytics

Durante l'utilizzo del Software, i seguenti dati verranno trasmessi automaticamente e regolarmente a Crashlytics per lo scopo dichiarato:

- ID software

- versione del software installato
- contrassegno indicante se il Software era in esecuzione in background
- architettura della CPU
- ID evento univoco
- data e ora dell'evento
- modello dispositivo
- spazio totale sul disco e quantità attualmente utilizzata
- nome e versione del sistema operativo
- RAM totale e quantità attualmente utilizzata
- contrassegno indicante se il dispositivo è collegato a un rooter
- orientamento dello schermo all'ora dell'evento
- prodotto/produttore hardware
- ID di installazione univoco
- versione delle statistiche inviate
- tipo di eccezione del Software
- testo del messaggio di errore
- un contrassegno indicante che l'eccezione del Software è stata causata da un'eccezione nidificata
- ID thread
- un contrassegno indicante se il frame è stato la causa dell'errore del Software
- un contrassegno indicante che il thread ha causato l'arresto imprevisto del Software
- informazioni sul segnale che ha causato l'arresto imprevisto del Software: nome del segnale, codice del segnale, indirizzo del segnale
- per ogni frame associato a un thread, un'eccezione o un errore: il nome del file di frame, il numero di riga del file di frame, i simboli di debug, l'indirizzo e l'offset nell'immagine binaria, il nome visualizzato della raccolta con il frame, il tipo di frame, il contrassegno indicante se il frame è stato la causa dell'errore
- ID sistema operativo
- ID del problema associato all'evento
- informazioni sugli eventi che si sono verificati prima che il Software si arrestasse in modo imprevisto: identificatore dell'evento, data e ora dell'evento, tipo e valore dell'evento;
- valori di registro CPU;

- tipo e valore dell'evento.

  I dati vengono inoltrati a Crashlytics tramite un canale protetto. Le informazioni sul trattamento dei dati da parte di Crashlytics sono disponibili su: https://firebase.google.com/terms/crashlytics-app-distribution-data-processing-terms.

La fornitura delle suddette informazioni a scopo di trattamento per finalità di marketing è volontaria.

Trasmissione dei dati in Kaspersky Security for iOS

Kaspersky Security for Mobile è conforme al Regolamento generale sulla protezione dei dati.

Per installare l'app, l'utente di un dispositivo deve leggere e accettare i termini delle seguenti informative relative all'elaborazione dei dati personali dell'utente:

- Contratto di licenza con l'utente finale
- Informativa sulla Privacy per Prodotti e Servizi

In alternativa, l'utente può leggere e accettare i termini della seguente informativa:

- Informativa di Kaspersky Security Network

L'utente può visualizzare i termini di questi documenti in qualsiasi momento nella sezione **Informazioni sull'app** → **Contratti e informative** nelle impostazioni di Kaspersky Security for iOS. In questa sezione l'utente può inoltre accettare o rifiutare i termini dell'Informativa KSN.

Scambio di informazioni con Kaspersky Security Network

Per migliorare la protezione in tempo reale, Kaspersky Security for iOS utilizza il servizio cloud Kaspersky Security Network per l'esecuzione del componente **Protezione Web**. L'app utilizza i dati ricevuti da KSN per esaminare le risorse Web prima dell'apertura.

Le informazioni sul tipo di dati inviati a Kaspersky durante l'utilizzo di KSN con Protezione Web sono disponibili nel Contratto di licenza con l'utente finale. Accettando i termini e le condizioni del Contratto di licenza, si accetta il trasferimento di queste informazioni.

Le informazioni sul tipo di dati statistici inviati a Kaspersky durante l'utilizzo di KSN con l'app mobile Kaspersky Security for iOS sono disponibili nell'Informativa di Kaspersky Security Network. Accettando i termini e le condizioni dell'Informativa, si accetta il trasferimento di queste informazioni.

Trasmissione dei dati nell'ambito del Contratto di licenza con l'utente finale

Se il Codice di attivazione viene usato per attivare il Software, al fine di verificare l'uso legittimo del Software, l'Utente finale accetta di fornire periodicamente al Titolare dei diritti le seguenti informazioni:

- Formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; indirizzo IPv4 del servizio Web a cui è stato eseguito l'accesso; dimensioni del contenuto della richiesta all'infrastruttura del Titolare dei diritti; ID protocollo; codice di attivazione del software; tipo di compressione dei dati; ID software; set di ID del Software che può essere attivato nel dispositivo dell'utente; localizzazione del software; versione completa del software; ID dispositivo univoco; data e ora nel dispositivo dell'utente; ID installazione Software (PCID); codice di

attivazione del software utilizzato attualmente; versione del sistema operativo, numero build del sistema operativo, numero di aggiornamento del sistema operativo, edizione del sistema operativo, informazioni estese sull'edizione del sistema operativo; modello dispositivo; codice del gestore di telefonia mobile; famiglia del sistema operativo; ID software derivato dalla licenza; elenco degli accordi presentati all'utente dal Software; tipo di contratto legale accettato dall'utente durante l'utilizzo del Software; versione del contratto legale accettato dall'utente durante l'utilizzo del Software; contrassegno indicante se l'utente ha accettato i termini del contratto legale durante l'utilizzo del Software; tipo di checksum per l'oggetto elaborato; intestazione licenza Software; ID di un centro di attivazione regionale; data e ora di creazione della chiave di licenza Software; ID della licenza Software; ID del modello di informazioni utilizzato per fornire la licenza Software; data e ora di scadenza della licenza Software; stato corrente della chiave di licenza Software; tipo di licenza Software utilizzata; tipo di licenza utilizzata per attivare il Software; ID software derivato dalla licenza;

Il Titolare dei diritti può utilizzare tali informazioni anche per la raccolta di dati statistici circa la distribuzione e l'uso del software del Titolare dei diritti.

Per proteggere il computer da minacce al sistema informatico, l'Utente finale accetta di fornire periodicamente al Titolare dei diritti le seguenti informazioni:

- Formato dei dati nella richiesta all'infrastruttura del Titolare dei diritti; indirizzo del servizio Web al quale è stato eseguito l'accesso (URL, IP); numero di porta; indirizzo Web dell'origine della richiesta del servizio Web (provenienza).

- versione completa del software; ID aggiornamento software; tipo di software installato; ID software; identificativo di configurazione; risultato dell'azione del Software; codice errore.

- Indirizzo Web in fase di elaborazione; indirizzo IPv4 del servizio Web a cui è stato eseguito l'accesso; identificazione personale del certificato digitale dell'oggetto esaminato e algoritmo hash; tipo di certificato; contenuti del certificato digitale elaborato.

Trasmissione dei dati nell'ambito dell'Informativa di Kaspersky Security Network

Quando l'Informativa KSN viene accettata, il Titolare dei diritti riceve automaticamente ed elabora i seguenti dati:

- Informazioni sulla qualità dei servizi KSN (protocollo utilizzato per lo scambio dati con KSN; ID del servizio KSN a cui ha avuto accesso il Software; data e ora di interruzione della ricezione di statistiche; numero di connessioni KSN provenienti dalla cache; numero di richieste per le quali è stata trovata una risposta nel database delle richieste locale; numero di connessioni KSN non riuscite; numero di transazioni KSN non riuscite; distribuzione temporanea delle richieste a KSN annullate; distribuzione temporanea delle connessioni KSN non riuscite; distribuzione temporanea delle transazioni KSN non riuscite; distribuzione temporanea delle connessioni KSN riuscite; distribuzione temporanea delle transazioni KSN riuscite; distribuzione temporanea delle richieste a KSN riuscite; distribuzione temporanea delle richieste a KSN in timeout; numero di nuove connessioni KSN; numero di richieste a KSN non riuscite a causa di errori di routing; numero di richieste non riuscite a causa della disattivazione di KSN nelle impostazioni del Software; numero di richieste a KSN non riuscite a causa di problemi di rete; numero di connessioni KSN riuscite; numero di transazioni KSN riuscite; numero totale di richieste KSN; data e ora di inizio ricezione delle statistiche).

- ID dispositivo; versione completa del software; ID aggiornamento software; ID installazione Software (PCID); tipo di software installato.

- Data e ora di installazione del Software; data di attivazione del software; localizzazione del software; contrassegno indicante se è abilitata la partecipazione a KSN; ID del software concesso in licenza; ID della licenza Software; ID sistema operativo; versione del sistema operativo installato nel computer dell'utente; versione del sistema operativo.

L'inserimento delle informazioni sopra indicate nel sistema KSN è facoltativo. È possibile scegliere di interrompere la partecipazione a Kaspersky Security Network in qualsiasi momento.

Contattare l'Assistenza tecnica

Questa sezione descrive come ottenere assistenza tecnica e le condizioni in base alle quali è disponibile.

Come ottenere assistenza tecnica

Se non è possibile trovare una soluzione al problema nella documentazione di Kaspersky Security for Mobile o in una delle fonti di informazioni su Kaspersky Security for Mobile, contattare l'Assistenza tecnica. Gli specialisti dell'Assistenza tecnica rispondono a tutti i quesiti in merito all'installazione e all'utilizzo di Kaspersky Security for Mobile.

Kaspersky fornisce il supporto di Kaspersky Security for Mobile durante il relativo ciclo di vita (vedere la pagina del ciclo di vita del supporto del prodotto). Prima di contattare l'Assistenza tecnica, consultare le regole dell'assistenza tecnica.

È possibile contattare l'Assistenza tecnica in uno dei seguenti modi:

- Visitando il sito Web dell'Assistenza tecnica
- Inviando una richiesta all'Assistenza tecnica tramite il portale Kaspersky CompanyAccount

Assistenza tecnica tramite Kaspersky CompanyAccount

Kaspersky CompanyAccount è un portale per le aziende che utilizzano le applicazioni Kaspersky. Il portale Kaspersky CompanyAccount è progettato per agevolare l'interazione tra gli utenti e gli specialisti di Kaspersky tramite richieste online. È possibile utilizzare Kaspersky CompanyAccount per tracciare lo stato delle richieste online e archiviarne una cronologia.

È possibile registrare tutti i dipendenti dell'organizzazione tramite un singolo account in Kaspersky CompanyAccount. Un singolo account consente di gestire in modo centralizzato le richieste in formato elettronico inviate a Kaspersky dai dipendenti registrati e di gestire i privilegi di tali dipendenti tramite Kaspersky CompanyAccount.

Il portale Kaspersky CompanyAccount è disponibile nelle seguenti lingue:

- Inglese
- Spagnolo
- Italiano
- Tedesco
- Polacco
- Portoghese
- Russo

- Francese
- Giapponese

Per ulteriori informazioni su Kaspersky CompanyAccount, visitare il sito Web dell'Assistenza tecnica.

Fonti di informazioni sull'applicazione

Pagina Web di Kaspersky Security for Mobile nel sito Web di Kaspersky

Nella pagina di Kaspersky Security for Mobile è possibile visualizzare informazioni generali sull'applicazione, le relative funzionalità e i parametri di esecuzione.

La pagina Web di Kaspersky Security for Mobile fornisce un collegamento al negozio online. Tramite il negozio online è possibile acquistare o rinnovare la licenza dell'applicazione.

Pagina Web di Kaspersky Security for Mobile nella Knowledge Base

La *Knowledge Base* è una sezione del sito Web del servizio di Assistenza tecnica.

Nella pagina di Kaspersky Security for Mobile nella Knowledge Base è possibile trovare articoli con informazioni utili, consigli e risposte alle domande frequenti sull'acquisto, l'installazione e l'utilizzo dell'applicazione.

Gli articoli della Knowledge Base forniscono risposte a domande relative non solo a Kaspersky Security for Mobile ma anche ad altre applicazioni Kaspersky. Possono inoltre includere notizie sul servizio di Assistenza tecnica.

Guida in linea

La guida in linea dell'applicazione comprende diversi file.

La guida sensibile al contesto dei plug-in di amministrazione per Kaspersky Security for Mobile fornisce informazioni sulle finestre di Kaspersky Security Center: una descrizione delle impostazioni di Kaspersky Security for Mobile e collegamenti alle descrizioni delle attività che utilizzano queste impostazioni.

La guida completa delle app Kaspersky Endpoint Security for Android e Kaspersky Security for iOS fornisce informazioni su come configurare e utilizzare le app mobili.

Discussione delle applicazioni Kaspersky nel Forum di supporto Kaspersky

Se la domanda non richiede una risposta immediata, è possibile sottoporla agli esperti di Kaspersky e ad altri utenti nel Forum.

Nel Forum è possibile visualizzare gli argomenti di discussione, pubblicare i propri commenti e creare nuovi argomenti di discussione.

Glossario

Abbonamento

Consente l'utilizzo dell'applicazione entro i parametri selezionati (data di scadenza e numero di dispositivi). È possibile sospendere o riprendere l'abbonamento, rinnovarlo automaticamente o annullarlo.

Administration Server

Un componente di Kaspersky Security Center che archivia in modo centralizzato le informazioni su tutte le applicazioni Kaspersky installate nei computer della rete. Può essere utilizzato anche per gestire tali applicazioni.

Amministratore di Kaspersky Security Center

La persona che gestisce le operazioni dell'applicazione tramite il sistema di amministrazione centralizzata remota di Kaspersky Security Center.

Amministratore dispositivo

Insieme dei diritti dell'app in un dispositivo Android che consentono all'app di utilizzare i criteri di gestione del dispositivo. È necessario implementare la funzionalità completa di Kaspersky Endpoint Security nei dispositivi Android.

Attivazione dell'applicazione

Passaggio dell'applicazione alla modalità con funzionalità complete. L'attivazione dell'applicazione viene eseguita dall'utente durante o dopo l'installazione dell'applicazione. Per attivare l'applicazione, è necessario disporre di un codice di attivazione o di un file chiave.

Attività di gruppo

Attività definita per un gruppo di amministrazione ed eseguita su tutti i dispositivi gestiti inclusi nel gruppo.

Categorie di Kaspersky

Categorie di dati predefinite sviluppate dagli esperti di Kaspersky. Le categorie possono essere aggiornate durante gli aggiornamenti dei database dell'applicazione. Un addetto alla sicurezza non può modificare o eliminare le categorie predefinite.

Certificato APN (servizio Apple Push Notification)

Certificato firmato da Apple, che consente di utilizzare il servizio Apple Push Notification. Tramite il servizio Apple Push Notification, un server MDM iOS può gestire i dispositivi iOS.

Codice di attivazione

Codice ricevuto al momento dell'acquisto di una licenza per Kaspersky Endpoint Security. Questo codice è richiesto per l'attivazione dell'applicazione.

Il codice di attivazione è una sequenza univoca di venti lettere e numeri nel formato xxxxx-xxxxx-xxxxx-xxxxx.

Codice di sblocco

Un codice che è possibile ottenere in Kaspersky Security Center. È necessario per sbloccare un dispositivo dopo l'esecuzione dei comandi **Blocca e localizza**, **Allarme** o **Foto utente** e all'attivazione di Auto-Difesa.

Contratto di licenza con l'utente finale

Accordo vincolante tra l'utente e AO Kaspersky Lab in cui vengono stipulate le condizioni per l'utilizzo dell'applicazione.

Controllo conformità

Verifica della conformità delle impostazioni di un dispositivo mobile e di Kaspersky Endpoint Security for Android ai requisiti di sicurezza aziendali. I requisiti di sicurezza aziendali disciplinano l'utilizzo del dispositivo. Ad esempio, la protezione in tempo reale deve essere abilitata nel dispositivo, i database anti-virus devono essere aggiornati e la password del dispositivo deve essere sufficientemente complessa. Controllo conformità si basa su un elenco di regole. Una regola di conformità include i seguenti componenti:

- Criterio di controllo del dispositivo (ad esempio l'assenza di app proibite nel dispositivo)
- Intervallo di tempo assegnato all'utente per correggere la mancata conformità (ad esempio 24 ore)
- Azione che verrà eseguita nel dispositivo se l'utente non corregge la mancata conformità entro il periodo di tempo definito (ad esempio il blocco del dispositivo)

Criterio

Set di impostazioni dell'applicazione e delle app mobili Kaspersky Endpoint Security applicate ai dispositivi nei gruppi di amministrazione o a singoli dispositivi. Diversi criteri possono essere applicati a differenti gruppi di amministrazione. Un criterio include le impostazioni configurate di tutte le funzioni delle app mobili Kaspersky Endpoint Security.

Database anti-virus

Database contenenti informazioni sulle minacce per la sicurezza del computer note a Kaspersky alla data di rilascio dei database anti-virus. Le voci nei database anti-virus consentono il rilevamento del codice dannoso negli oggetti esaminati. I database anti-virus vengono creati dagli esperti di Kaspersky e aggiornati ogni ora.

Dispositivo EAS

Dispositivo mobile connesso ad Administration Server tramite il protocollo Exchange ActiveSync.

Dispositivo MDM iOS

Dispositivo mobile iOS controllato dal server MDM iOS.

Dispositivo supervisionato

Dispositivo iOS le cui impostazioni sono monitorate da Apple Configurator, un programma per la configurazione di gruppo dei dispositivi iOS. Un dispositivo supervisionato ha lo stato *controllato* in Apple Configurator. Ogni volta che un dispositivo supervisionato si collega al computer, Apple Configurator verifica la configurazione del dispositivo rispetto alle impostazioni di riferimento specificate e le ridefinisce, se necessario. Un dispositivo supervisionato non può essere sincronizzato con Apple Configurator installato in un altro computer.

Ogni dispositivo supervisionato fornisce più impostazioni da ridefinire tramite il criterio di Kaspersky Device Management for iOS rispetto a un dispositivo non supervisionato. È ad esempio possibile configurare un server proxy HTTP per il monitoraggio del traffico Internet in un dispositivo all'interno della rete aziendale. Per impostazione predefinita, tutti i dispositivi mobili non sono supervisionati.

File chiave

Un file in formato xxxxxxxx.key che consente l'utilizzo di un'applicazione Kaspersky con una licenza commerciale o di prova. L'applicazione genera il file chiave in base al codice di attivazione. È possibile utilizzare l'applicazione solo quando si dispone di un file chiave.

File manifesto

File in formato PLIST che contiene un collegamento al file dell'app (file ipa) presente in un server Web. È utilizzato dai dispositivi iOS per localizzare, scaricare e installare le app da un server Web.

Gruppo di amministrazione

Set di dispositivi gestiti, ad esempio dispositivi mobili raggruppati in base alle relative funzioni, e il set di app installate in tali dispositivi. I dispositivi gestiti sono raggruppati in modo da poter essere amministrati come una singola unità. Ad esempio, i dispositivi mobili che eseguono lo stesso sistema operativo possono essere combinati in un gruppo di amministrazione. Un gruppo può contenere altri gruppi di amministrazione. È possibile creare attività e criteri di gruppo per i dispositivi di un gruppo.

IMAP

Protocollo per l'accesso all'e-mail. A differenza del protocollo POP3, IMAP fornisce funzionalità estese per l'utilizzo delle cassette postali, ad esempio la gestione delle cartelle e dei messaggi senza copiarne il contenuto dal server di posta. Il protocollo IMAP utilizza la porta 134.

Kaspersky Private Security Network (KSN Privato)

Kaspersky Private Security Network è una soluzione che offre agli utenti dei dispositivi con applicazioni Kaspersky installate l'accesso ai database di reputazione di Kaspersky Security Network e ad altri dati statistici, senza l'invio dei dati dai propri dispositivi a Kaspersky Security Network. Kaspersky Private Security Network è progettato per i clienti aziendali che non sono in grado di partecipare a Kaspersky Security Network per uno dei seguenti motivi:

- I dispositivi degli utenti non sono connessi a Internet.
- La trasmissione dei dati al di fuori del paese o della LAN aziendale è vietata dalla legge o dai criteri di protezione aziendale.

Kaspersky Security Network (KSN)

Un'infrastruttura di servizi cloud che consente l'accesso al database Kaspersky con informazioni costantemente aggiornate sulla reputazione di file, risorse Web e software. Kaspersky Security Network garantisce una risposta più rapida da parte delle applicazioni Kaspersky alle minacce, migliora le prestazioni di alcuni componenti di protezione e riduce la probabilità di falsi positivi.

Licenza

Un diritto limitato nel tempo di utilizzare l'app, concesso in base al Contratto di licenza con l'utente finale.

Pacchetto di installazione

Set di file creati per l'installazione remota di un'applicazione Kaspersky tramite un sistema di amministrazione remota. Viene creato un pacchetto di installazione sulla base dei file dedicati inclusi nel pacchetto di distribuzione dell'applicazione. Il pacchetto di installazione contiene una serie di impostazioni necessarie per installare l'applicazione e renderla immediatamente operativa dopo l'installazione. I valori delle impostazioni nel kit di distribuzione corrispondono ai valori predefiniti delle impostazioni dell'applicazione.

Pacchetto di installazione indipendente

File di installazione di Kaspersky Endpoint Security per il sistema operativo Android, che contiene le impostazioni per la connessione dell'applicazione ad Administration Server. Viene creato in base al pacchetto di installazione dell'applicazione ed è un caso particolare di pacchetto di app mobili.

Periodo di validità della licenza

Periodo di tempo durante il quale l'utente ha accesso alle funzionalità dell'applicazione e dispone dei diritti per l'utilizzo di servizi aggiuntivi. I servizi che è possibile utilizzare dipendono dal tipo di licenza.

Phishing

Un tipo di frode su Internet volta a ottenere l'accesso non autorizzato ai dati riservati degli utenti.

Plug-in di gestione dell'applicazione

Componente dedicato che fornisce l'interfaccia per la gestione delle applicazioni Kaspersky tramite Administration Console. Ogni applicazione che può essere gestita tramite Kaspersky Security Center SPE dispone di uno specifico plug-in di amministrazione. Il plug-in di amministrazione è incluso in tutte le applicazioni Kaspersky Lab che possono essere gestite tramite Kaspersky Security Center.

POP3

Protocollo di rete utilizzato da un client di posta per ricevere messaggi da un server di posta.

Profilo di provisioning

Raccolta di impostazioni per il funzionamento delle applicazioni nei dispositivi mobili iOS. Un profilo di provisioning contiene le informazioni sulla licenza; è collegato a un'applicazione specifica.

Profilo lavoro Android

Un ambiente sicuro nel dispositivo dell'utente in cui l'amministratore può gestire app e account utente senza limitare l'utilizzo dei dati personali da parte dell'utente. Quando nel dispositivo mobile dell'utente viene creato un profilo lavoro, in quest'ultimo vengono automaticamente installate le seguenti app aziendali: Google Play Market, Google Chrome, Download, Kaspersky Endpoint Security for Android e così via. Le app aziendali installate nel profilo lavoro e le notifiche di tali app sono contrassegnate con un'icona rossa a forma di valigetta. È necessario creare un account aziendale Google separato per l'account Google Play Market. Le app installate nel profilo lavoro vengono visualizzate nell'elenco standard delle app.

Profilo MDM iOS

Profilo con una serie di impostazioni per la connessione dei dispositivi mobili iOS all'Administration Server. Un profilo MDM iOS consente di distribuire profili di configurazione iOS in background tramite il server MDM iOS e di ricevere informazioni diagnostiche dettagliate sui dispositivi mobili. Un collegamento al profilo MDM iOS deve essere inviato a un utente per consentire il rilevamento e la connessione del dispositivo mobile iOS dell'utente da parte del server MDM iOS.

Quarantena

Cartella in cui l'applicazione Kaspersky sposta gli oggetti potenzialmente infetti che sono stati rilevati. Gli oggetti vengono archiviati in Quarantena in forma criptata al fine di evitare qualsiasi impatto sul computer.

Richiesta di firma del certificato

File con le impostazioni di un Administration Server, che viene approvato da Kaspersky e quindi inviato ad Apple per ottenere un certificato APNs.

Server degli aggiornamenti Kaspersky

Server HTTP(S) di Kaspersky da cui le applicazioni Kaspersky scaricano gli aggiornamenti dei moduli dell'applicazione e dei database.

Server MDM iOS

Un componente di Kaspersky Endpoint Security installato in un dispositivo client che consente la connessione dei dispositivi mobili iOS ad Administration Server e la gestione dei dispositivi mobili iOS tramite il servizio APNs (Apple Push Notifications).

Server per dispositivi mobili Exchange

Un componente di Kaspersky Endpoint Security che consente di connettere i dispositivi mobili Exchange ActiveSync ad Administration Server.

Server proxy

Un servizio di rete del computer che consente agli utenti di inoltrare richieste indirette ad altri servizi di rete. In primo luogo, un utente si connette a un server proxy e richiede una risorsa (ad esempio un file) situata in un altro server. A questo punto il server proxy si connette al server specificato e ne ottiene la risorsa desiderata oppure restituisce la risorsa dalla propria cache (qualora il proxy ne disponga). In alcuni casi, la richiesta di un utente o la risposta di un server può essere modificata dal server proxy per determinati motivi.

Server Web di Kaspersky Security Center

Componente di Kaspersky Security Center installato insieme ad Administration Server. Il Server Web è progettato per la trasmissione, tramite una rete, di pacchetti di installazione indipendenti, profili MDM iOS e file da una cartella condivisa.

SSL

Un protocollo di criptaggio dei dati utilizzato in Internet e nelle reti locali. Il protocollo SSL (Secure Sockets Layer) è utilizzato nelle applicazioni Web per creare una connessione sicura tra un client e un server.

Virus

Un programma che ne infetta altri aggiungendovi il proprio codice per ottenere il controllo al momento dell'esecuzione dei file infetti. Questa semplice definizione consente di identificare l'azione principale eseguita da qualsiasi virus: l'infezione.

Workstation dell'amministratore

Il computer in cui è stato distribuito Kaspersky Security Center Administration Console. Se il plug-in di amministrazione dell'applicazione è installato nella workstation di amministrazione, l'amministratore può gestire le app mobili Kaspersky Endpoint Security distribuite nei dispositivi degli utenti.

Informazioni sul codice di terze parti

È possibile scaricare e leggere informazioni sul codice di terze parti nei seguenti file:

- legal_notices_Android.txt (per l'app Kaspersky Endpoint Security for Android)
- legal_notices_iOS.txt (per l'app Kaspersky Security for iOS)

Nei dispositivi mobili le informazioni sul codice di terze parti sono disponibili nella sezione **Informazioni sull'app** delle app mobili.

Note sui marchi

I marchi registrati e i marchi di servizi sono di proprietà dei rispettivi titolari.

PostScript è un marchio o un marchio registrato di Adobe negli Stati Uniti e/o in altri paesi.

AirDrop e AirPrint sono marchi di Apple Inc.

Apple, Apple Configurator, AirPlay, AirPort Express, App Store, Apple TV, Bonjour, Face ID, FaceTime, FileVault, iBooks, iCal, iCloud, iPad, iPadOS, iPhone, iTunes, OS X, Safari, Spotlight e Touch ID sono marchi di Apple Inc., registrati negli Stati Uniti e in altri paesi e aree geografiche.

Aruba Networks è un marchio di Aruba Networks, Inc. registrato negli Stati Uniti e in altri paesi.

La parola, il marchio e i loghi Bluetooth sono di proprietà di Bluetooth SIG, Inc.

Cisco, Cisco AnyConnect e IOS sono marchi o marchi registrati di Cisco Systems, Inc. e/o delle relative consociate negli Stati Uniti e in altri paesi.

SecurID è un marchio o un marchio registrato di EMC Corporation registrato negli Stati Uniti e/o in altri paesi.

Google, Android, Chrome, Chromebook, Chromium, Crashlytics, Firebase, Google Analytics, Google Chrome, Google Mail, Google Maps, Google Play, Nexus e SPDY sono marchi di Google LLC.

HTC è un marchio di HTC Corporation.

Huawei, HUAWEI ed EMUI sono marchi di Huawei Technologies Co., Ltd registrati in Cina e in altri paesi.

IBM e Maas360 sono marchi di International Business Machines Corporation, registrati in molte giurisdizioni in tutto il mondo.

Juniper Networks, Juniper e JUNOS sono marchi o marchi registrati di Juniper Networks, Inc. negli Stati Uniti e in altri paesi.

Microsoft, ActiveSync, Microsoft Intune, Tahoma, Windows, Windows Mobile e Windows Phone sono marchi del gruppo di aziende Microsoft.

MOTOROLA e il logo M stilizzato sono marchi o marchi registrati di Motorola Trademark Holdings, LLC.

Oracle, JavaScript sono marchi registrati di Oracle e/o delle relative consociate.

Il marchio BlackBerry appartiene a Research In Motion Limited, è registrato negli Stati Uniti e potrebbe essere in sospeso o registrato in altri paesi.

Samsung è un marchio di SAMSUNG negli Stati Uniti e in altri paesi.

SonicWALL, Aventail e SonicWALL Mobile Connect sono marchi di SonicWall, Inc.

SOTI e MobiControl sono marchi registrati di SOTI Inc. negli Stati Uniti e in altre giurisdizioni.

Symantec è un marchio o un marchio registrato di Symantec Corporation o delle relative consociate negli Stati Uniti e in altri paesi.

Il marchio Symbian è di proprietà di Symbian Foundation Ltd.