SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

Guida in linea (Android)

Versione prodotto: 9.6

Sommario

1 Accessibilità

Sophos Intercept X for Mobile è conforme alle Web Content Accessibility Guidelines (WCAG) 2.1, livello AA. Ulteriori informazioni su queste linee guida sono disponibili nelle informazioni correlate.

Si consiglia di utilizzare Sophos Intercept X for Mobile con TalkBack, il lettore di schermo di Google, integrato nei dispositivi Android. Il link per l'utilizzo di TalkBack è reperibile nelle informazioni correlate. Per ulteriore assistenza con TalkBack, contattare il supporto tecnico di Google.

Se si desidera utilizzare prodotti con tecnologia assistiva insieme al nostro software, si consiglia di acquisire familiarità con il funzionamento del prodotto selezionato e con i comandi della tastiera disponibili.

Limitazione nota

A causa di una limitazione del sistema operativo Android, gli utenti che adoperano lettori di schermo in Android 9 o versioni successive possono utilizzare solamente le intestazioni per navigare.

Informazioni correlate

Web Content Accessibility Guidelines

Guida di Accessibilità Android: Guida introduttiva a TalkBack su Android

2 Informazioni su Sophos Intercept X for Mobile

Sophos Intercept X for Mobile protegge i dispositivi Android nel massimo rispetto della privacy, senza incidere negativamente su performance e durata della batteria. Grazie all'aggiornamento minuto per minuto dei dati di intelligence dei SophosLabs, le app vengono automaticamente sottoposte a scansione antimalware in fase di installazione, per proteggervi contro il rischio di perdita dei dati e i costi inattesi che ne potrebbero derivare.

3 Pannello di controllo

Il pannello di controllo di Sophos Intercept X for Mobile fornisce un quadro generale dello stato del dispositivo.

Le funzionalità hanno colori diversi a seconda del relativo stato:

- Verde: Nessun problema rilevato
- Rosso: Problemi individuati
- Blu: La funzionalità è attivata
- Grigio: La funzionalità è disattivata o non configurata

4 Sicurezza dei dispositivi

Come tutti i sistemi operativi, Android permette di configurare impostazioni che hanno ripercussioni sulla sicurezza del dispositivo. Sophos Intercept X for Mobile controlla queste impostazioni relative alla protezione e fornisce consigli per incrementare la sicurezza del dispositivo.

Nota
Quando Sophos Intercept X for Mobile è gestita da Sophos Mobile, le impostazioni di sistema inerenti alla sicurezza vengono configurate dall'organizzazione.

Le impostazioni elencate sotto **Sicurezza dei dispositivi** hanno colori diversi a seconda del relativo stato:

- Verde (protetto): questa impostazione garantisce la massima protezione possibile per il dispositivo.
- Rosso (non protetto): questa impostazione potrebbe causare problemi di sicurezza. Seguire le raccomandazioni fornite per modificarla.
- Giallo (sconosciuto): i dispositivi Android hanno impostazioni diverse a seconda del modello del dispositivo e della versione di Android. Qualora Sophos Intercept X for Mobile non fosse in grado di determinare se l'impostazione è pericolosa, verrà visualizzata in giallo. Si consiglia di modificarla.
- Grigio (disattivato): La verifica è disattivata. Questa impostazione non viene presa in considerazione per determinare lo stato di sicurezza del dispositivo.

Toccare un'impostazione per modificarla o per ulteriori informazioni sul suo impatto sulla protezione del dispositivo.

4.1 Update Advisor

Update Advisor mostra informazioni sulla versione di Android utilizzata e verifica se siano disponibili versioni più recenti.

Update Advisor utilizza le statistiche di installazione per scoprire se sia disponibile una nuova versione di Android per il dispositivo.

Per aprire Update Advisor, selezionare **Ultima versione di Android** nella pagina **Sicurezza dei dispositivi**.

Si consiglia di attivare l'installazione automatica degli aggiornamenti. Se nel dispositivo è presente un'impostazione opzionale per questa operazione, toccare **Verifica impostazioni** e attivare gli aggiornamenti automatici nell'app **Impostazioni** del dispositivo.

5 Filtro web

Il Filtro web serve a specificare i tipi di siti web per cui si desidera ricevere avvisi prima della loro apertura. Questa opzione consente di impedire agli utenti di visitare siti con contenuti malevoli, inappropriati o illegali.

Configurazione del filtro web

Nella dashboard, il Filtro web è disponibile sotto **Protezione della rete**.

- Nella pagina **Filtro web**, attivare il Filtro web.
- Per abilitare il filtro dei siti web malevoli, toccare **Contenuti malevoli** e selezionare **Avvisa** o **Blocca**.
- Per abilitare il filtro dei siti web che rientrano in una categoria specifica, toccare la categoria e selezionare la voce **Avvisa** o **Blocca**.
- **Elenco Consenti:** è possibile eliminare permanentemente gli avvisi relativi a pagine malevole o facenti parte di determinate categorie di filtro. Questa funzionalità è particolarmente utile se si accede con frequenza a pagine che rientrano in una categoria che invia notifiche o viene bloccata automaticamente. Selezionare l'opzione **Autorizza sempre l'accesso a questa pagina** nella finestra di avviso **Web Filtering**. Per filtrare nuovamente tali pagine, toccare **Cancella l'elenco delle pagine consentite**.

Consiglio
Per testare il filtro web, Sophos ha creato il sito sophostest.com, che contiene pagine di prova per ciascuna categoria. Sebbene alcune di queste pagine siano classificate come potenzialmente offensive o pericolose, i contenuti delle pagine stesse sono innocui in tutti i casi.

Browser Web supportati

Il Filtro web protegge gli utenti quando viene utilizzata una delle app elencate in **Browser protetti**.

Browser supportati:

- Google Chrome
- Firefox
- Browser web per Android
- Microsoft Edge

In **Browser protetti (non verificati)**, vengono elencate le app che potrebbero funzionare, ma la cui compatibilità non è stata verificata.

Consiglio
Se un browser web supportato viene installato nel dispositivo ma non viene elencato sotto **Browser protetti**, verificare che Sophos Accessibility Service sia attivo (nelle impostazioni di sistema, sotto **Accessibilità**).

6 Link Checker

Link Checker serve a verificare i link inclusi nelle e-mail o nei documenti, per rilevare contenuti malevoli o inappropriati.

Link Checker elabora tutti i link selezionati nelle app non categorizzate come browser. Il Filtraggio web serve invece a verificare i link all'interno di una pagina web. Vedere Filtro web (pagina 5).

Nella dashboard, Link Checker è disponibile sotto **Protezione della rete**.

Per impostare Link Checker:

1. Nella pagina **Link Checker**, attivare Link Checker.
2. Selezionare la consueta app browser per l'apertura dei link web.
3. La prima volta che si seleziona un link dopo l'attivazione di Link Checker, Android chiederà di selezionare un'app per l'apertura del link. Selezionare **Sophos Link Checker**.

Quando si seleziona un link, quest'ultimo verrà inoltrato a Link Checker e analizzato per rilevare l'eventuale presenza di contenuti malevoli o inappropriati, secondo la classificazione fornita dai SophosLabs. Successivamente, il link verrà aperto nel browser.

Nota
Link Checker non è in grado di verificare i link nelle app che, invece di inoltrarli all'app browser, aprono i link internamente. Se l'app consente di scegliere la modalità di apertura dei link web, selezionare il browser per permettere a Link Checker di elaborare i link.

Per esempio, in Gmail questa impostazione si chiama **Apri link web in Gmail**. Disattivare questa impostazione per consentire a Link Checker di verificare i link contenuti nei messaggi e-mail.

7 Protezione Wi-Fi

La protezione Wi-Fi serve a verificare la connessione Wi-Fi per rilevare la presenza di eventuali minacce di rete.

Nota
Se Sophos Intercept X for Mobile è registrata a Sophos Mobile, questa funzionalità viene gestita dall'organizzazione.

Sulla dashboard, la protezione Wi-Fi è disponibile sotto **Protezione della rete**.

Tipi di problemi

Sophos Intercept X for Mobile rileva i seguenti problemi:

Spoofing dell'ARP	Lo spoofing dell'ARP si verifica quando l'autore di un attacco invia messaggi ARP (Address Resolution Protocol) al computer, per indurlo a credere che l'indirizzo MAC dell'autore dell'attacco sia associato all'indirizzo IP del gateway di rete. Questo stratagemma consente ai cybercriminali di infiltrarsi nella rete privata, prelevare dati di natura sensibile e lanciare altri attacchi come quelli di tipo denial-of-service o man-in-the-middle.
Captive portal	I captive portal vengono utilizzati nelle reti Wi-Fi pubbliche per richiedere l'autenticazione prima di concedere accesso alla rete. Poiché l'intero traffico viene reindirizzato sul captive portal, potrebbero essere visualizzati altri avvisi.
Manipolazione dei contenuti	La manipolazione dei contenuti si verifica quando l'autore di un attacco manipola i contenuti di un sito web per costringere l'utente a svolgere operazioni dannose. Questo stratagemma permette ai cybercriminali di riuscire, ad esempio, a bypassare l'autenticazione o eliminare i dati.
Intercettazione SSL	L'intercettazione SSL si verifica quando l'autore di un attacco adopera un falso certificato del server per intercettare la connessione sicura tra il computer e un sito web. L'autore dell'attacco è in grado di decifrare i dati di natura sensibile, mentre l'utente pensa di utilizzare una connessione sicura.
Rimozione dell'SSL	La rimozione dell'SSL si verifica quando l'autore di un attacco modifica la connessione di un sito web, portandola da una connessione HTTPS protetta a una connessione HTTP non protetta. L'autore dell'attacco è in grado di inoltrare sul proprio server proxy l'intero traffico tra il computer

e il sito web. Questo stratagemma consente ai cybercriminali di decifrare i dati di natura sensibile, mentre l'utente pensa di essere ancora connesso tramite HTTPS.

Test

- Per verificare la rete Wi-Fi a cui si è connessi, toccare **Verifica Wi-Fi**.
- Per effettuare test della rete in background, attivare **Test in background**. Attivando questa opzione, verrà effettuato un test ogni volta che il dispositivo si connette a una rete Wi-Fi.

8 Sicurezza delle app

Il dispositivo può essere sottoposto a scansione, per individuare eventuali app o file malevoli.

Sophos Intercept X for Mobile effettua la scansione del dispositivo alla ricerca di malware, segnalando e comunicando la presenza di eventuali app malevole o potenzialmente indesiderate. La funzione di scansione effettua ricerche on-line per confrontare le nuove app con i dati sulle minacce presenti sia nel database in-the-cloud dei SophosLabs che nel motore di rilevamento delle minacce integrato e a funzionalità complete, con l'obiettivo di garantire valori di rilevamento sempre migliori sia in modalità on-line che off-line. I dati dell'antivirus vengono costantemente aggiornati dai SophosLabs, che analizzano le minacce Android 24 ore su 24.

Esecuzione di scansioni

Sophos Intercept X for Mobile sottopone automaticamente a scansione le app in fase di installazione. Inoltre, è possibile configurare scansioni pianificate ed eseguire scansioni manuali.

Per configurare scansioni pianificate:

Nelle impostazioni dell'app, selezionare **Scansioni pianificate** e successivamente selezionare un intervallo di scansione sotto **Intervalli della scansione pianificata**. È anche possibile configurare quali parti del dispositivo debbano essere sottoposte a scansione e quali tipi di app debbano essere segnalati.

Per eseguire una scansione manuale:

Nella pagina **Sicurezza delle app**, selezionare **Mostra dettagli scansione** e successivamente **Avvia**.

Visualizzazione dei risultati della scansione

Nella pagina **Sicurezza delle app**, viene visualizzata una panoramica dei risultati della scansione sotto **Problemi di sicurezza delle app**.

Per visualizzare i singoli problemi, selezionare **Mostra dettagli scansione**.

Per visualizzare ulteriori dettagli su un problema, selezionare un'app elencata sotto **Minacce e PUA**, per aprirne la pagina **Dettagli oggetto**. In questa pagina è possibile svolgere le seguenti operazioni:

- Visualizzare com'è stata installata l'app e quali autorizzazioni ha richiesto.
- Visualizzare una descrizione della minaccia.
- Aprire nel browser una pagina web con informazioni dettagliate sulla minaccia.
- Disinstallare l'app.
- Autorizzare l'app.

Riferimenti correlati

impostazioni (pagina 23)

9 Autenticatore

L’Autenticatore serve a generare password one-time (dette anche codici di verifica) per l’accesso ad account che utilizzano l’autenticazione a fattori multipli.

Verificare che l'autenticazione a fattori multipli sia supportata dal provider dell’account, e in tal caso controllare come abilitarla per il proprio account.

L’Autenticatore supporta password con accesso **a tempo** e con accesso **basato su contatore**. Vedere Informazioni sulle password one-time (pagina 10).

Per avviare l'Autenticatore, toccare e tenere premuta l'icona Sophos e successivamente toccare **Autenticatore**.

Funzionalità:

- Per le password **a tempo**, l’Autenticatore visualizza la password one-time attualmente in uso, con un’icona animata che raffigura il tempo di validità rimanente del codice attuale, allo scadere del quale verrà calcolato il codice successivo.
- Per le password **basate su contatore**, toccare **Aggiorna** accanto all’account desiderato per generare una nuova password one-time. Per prevenire la generazione involontaria di codici multipli consecutivi, vi è una latenza che prevede un’attesa di alcuni secondi dopo ciascuna generazione, prima che sia possibile richiedere il codice successivo.
- Per copiare negli appunti l’attuale password one-time di un account, toccare e tenere premuto l’account desiderato, e successivamente selezionare **Copia**.
- Per modificare i dettagli dell’account, toccare e tenere premuto l’account desiderato, e selezionare **Modifica**. Per questioni di sicurezza, non è possibile visualizzare o modificare la chiave segreta.
- Per eliminare un account, toccare e tenere premuto l’account desiderato, e selezionare **Elimina**.

Avviso
Quando si elimina una voce Autenticatore, viene eliminata anche la possibilità di generare password one-time per l'account in questione. Questa azione non disattiva l’autenticazione a fattori multipli. L'eliminazione della voce Autenticatore potrebbe impedire l'accesso al proprio account.

Prima di eliminare una voce, verificare di disporre di un meccanismo alternativo per generare password one-time oppure di un modo per poter accedere all'account senza l'autenticazione a fattori multipli.

9.1 Informazioni sulle password one-time

Le password one-time (note anche come codici di verifica) sono composte da una serie di numeri. Vengono calcolate utilizzando i seguenti parametri:

- Una chiave segreta condivisa, nota solamente al provider dell’account e all’utente.
- Valori di configurazione specifici del provider dell'account.
- Un contatore a sequenza.

Quando si utilizza una password one-time per effettuare l'autenticazione, il provider dell'account attende una password che viene calcolata in base a un valore specifico del contatore. Siccome

l'Autenticatore utilizza le stesse regole del provider dell'account per determinare il valore attuale del contatore, il provider accetterà la password one-time.

L'Autenticatore supporta password con accesso **a tempo** e con accesso **basato su contatore**. Queste tipologie differiscono nel modo in cui viene determinato il valore corrente del contatore:

- **Password one-time a tempo** (TOTP, secondo lo standard RFC 6238): Il valore del contatore viene costantemente incrementato in base all'ora corrente. Il valore successivo nella serie di codici di verifica viene generato una volta trascorso un periodo di tempo predefinito.
- **Password one-time basate su contatore** (HOTP, secondo lo standard RFC 4226): Il valore del contatore viene incrementato con ciascuna richiesta ricevuta. Il valore successivo nella serie di codici di verifica viene generato su richiesta.

9.2 Aggiunta di un account dal codice QR

Utilizzare questa procedura se è stata abilitata l'autenticazione a fattori multipli per un account e il provider dell'account ha fornito un codice QR contenente i dettagli di configurazione.

1. Toccare **+** e successivamente **Scansione del codice QR**.
2. Scannerizzare il codice QR con il dispositivo.

Una volta che l'app ha letto i dettagli di configurazione dal codice QR, imposterà un nuovo account Autenticatore.

9.3 Aggiunta manuale di un account

Utilizzare questa procedura se è stata abilitata l'autenticazione a fattori multipli per un account, e il provider dell'account ha fornito un elenco di dettagli di configurazione.

1. Toccare **+** e successivamente **Aggiungi manualmente**.
2. Nel campo **Nome**, digitare un nome per il nuovo account Autenticatore.
3. Nel campo **Chiave**, digitare la chiave segreta specificata dal provider dell'account. La chiave è valida solo per l'account interessato, e costituisce la base utilizzata per calcolare le password one-time.
4. Nel campo **Tipo**, selezionare il tipo di calcolo specificato dal provider dell'account.
5. Se il provider dell'account ha specificato impostazioni aggiuntive, toccare **Opzioni avanzate** per visualizzare ulteriori campi di immissione.

Attenzione
Compilare solamente i campi per i quali il provider dell'account ha specificato informazioni da inserire.

- Nel campo **Autorità emittente**, inserire una stringa che indichi il provider a cui è associato l'account.
- Nel campo **Periodo di tempo**, inserire il periodo di validità in secondi. Disponibile solamente per password one-time a tempo.
- Nel campo **Contatore**, inserire il numero iniziale per il contatore. Disponibile solamente per password basate su contatore.
- Nel campo **Lunghezza del codice**, selezionare il numero di cifre per le password one-time.

- Nel campo **Algoritmo hash**, selezionare l’algoritmo hash per il calcolo delle password one-time.

6. Richiesto: Nel campo **Colore sfondo**, selezionare un colore da assegnare alla voce corrispondente all’account, per semplificarne l’individuazione nell’elenco degli account.
7. Una volta pronti per continuare, toccare **OK** ✓.

Questa procedura imposterà un nuovo account Autenticatore.

10 Password Safe

Password Safe serve a memorizzare tutti i dati dell'account in un unico posto, protetto da una password master.

Per avviare Password Safe, toccare e tenere premuta l'icona Sophos e successivamente toccare **Password Safe**.

Esistono le seguenti opzioni:

- Crea un nuovo file Password Safe.
- Importa un file KeePass KDBX già esistente. Quando si modificano voci della password, verrà modificata solamente la copia locale.

Attivazione della funzionalità Riempimento automatico

Su iOS 12 e versioni successive è possibile utilizzare Password Safe per il riempimento automatico delle password.

Per attivare il **Riempimento automatico** per Password Safe:

1. Aprire l'app **Impostazioni** e scorrere verso il basso fino a **Password e account**.
2. Toccare **Riempimento automatico** e attivare **Riempimento automatico**.
3. Selezionare **Intercept X** sotto **Consenti riempimento da:**.

È ora possibile accedere a Password Safe semplicemente toccando **Password** sulla barra QuickType sopra la tastiera, quando viene richiesto l'inserimento delle credenziali.

10.1 Creazione di una voce Password Safe

Per aggiungere una voce o un gruppo di voci a un file Password Safe:

1. In Password Safe, toccare **+**.
2. Selezionare il tipo di voce che si desidera creare:
   - **Aggiungi voce account** crea una voce con campi predefiniti che possono essere utilizzati per account web ed elementi simili.
   - **Aggiungi voce carta di credito** crea una voce con campi predefiniti che possono essere utilizzati per carte di credito ed elementi simili.
   - **Aggiungi gruppo** crea una cartella all'interno della Password Safe per organizzare le voci.
3. Immettere i dati nei campi della voce.
4. Richiesto: Toccare **Aggiungi campo** per aggiungere un campo personalizzato alla voce.

   Se si attiva **Protetto** per un campo personalizzato, è necessario toccare il pulsante a forma di occhio accanto al campo desiderato, per visualizzarne il valore. Inoltre, i campi protetti sono esclusi dai risultati di ricerca.
5. Toccare l'icona a forma di **Dischetto** per salvare la voce.

I dati della password possono essere utilizzati per accedere in maniera semplice e veloce a una pagina web o a un'app. Vedere Utilizzo dei dati delle password per effettuare l'accesso (pagina 14).

10.2 Generazione di password

1. Aprire la voce Password Safe per la quale si desidera generare una password.
2. Toccare **Modifica** per passare alla modalità di modifica.
3. Toccare **+** accanto al campo della password per aprire il generatore di password.
4. Definire la lunghezza della password e i tipi di carattere che devono essere inclusi nella password.
5. Toccare **Genera password** per generare una password secondo i criteri specificati.
6. Una volta generata una password che soddisfa i propri requisiti, chiudere il generatore di password. La password viene aggiornata con il valore generato.
7. Salvare la voce.

10.3 Utilizzo dei dati delle password per effettuare l'accesso

- Per copiare il valore di un campo negli Appunti, toccare il campo richiesto.
- Per visualizzare il valore dei campi protetti, toccare l'icona a forma di **Occhio** accanto al campo protetto.
- Per aprire un URL nel browser web, toccare l'URL. Se si desidera invece copiare l'URL negli Appunti, toccare e tenere premuto l'URL desiderato.

Consiglio
Ogni volta che si apre una voce Password Safe, viene aggiunta una notifica all'area di notifica di Android. Da questa notifica è possibile copiare negli appunti i valori di nome utente e password.

10.4 Gestione delle voci di Password Safe

1. Toccare e tenere premuta una voce per passare alla modalità di selezione.
2. Richiesto: Selezionare altre voci per le quali si desidera svolgere la stessa azione.
3. Toccare un'icona per effettuare l'azione desiderata:
   - **Modifica**: Modificare i contenuti della voce. Disponibile solamente quando è selezionata solo una voce.
   - **Taglia**: Trasferire le voci selezionate in un altro gruppo all'interno del file Password Safe.
   - **Copia**: Copiare le voci selezionate in un altro gruppo all'interno del file Password Safe.
   - **Elimina**: Trasferire le voci selezionate nel gruppo speciale **Cestino**. Per eliminare le voci in modo permanente, utilizzare l'opzione **Elimina** per le voci nel gruppo **Cestino**.
   - Per incollare una voce che è stata tagliata o copiata, selezionare il percorso di destinazione e toccare **Appunti**.

10.5 Ricerca di voci di Password Safe

In Password Safe è possibile cercare voci e nomi di gruppi, oppure valori dei campi delle voci.

Nota
Non è possibile cercare campi password o campi configurati come **Protetti**.

1. In Password Safe, toccare **Cerca** per passare alla modalità di ricerca.
2. Inserire una stringa di ricerca. L'elenco dei risultati viene aggiornato man mano che si digitano lettere.

10.6 Backup di Password Safe

È importante effettuare regolarmente backup del file Password Safe. Se si dovesse perdere il file Password Safe, ad esempio in caso di formattazione non intenzionale o smarrimento del dispositivo, non sarà possibile accedere ai dati della password, a meno che non si disponga di una copia di backup recente.

1. In Password Safe, toccare **Altro** e successivamente **Esporta**.
2. Selezionare l’app nella quale si desidera esportare il file Password Safe.
   Una copia del file Password Safe verrà condivisa con l’app selezionata.

Nota
Si consiglia di annotare il percorso della copia di backup e di conservare il foglio in un luogo sicuro.

11 Scansione del codice QR

La scansione del codice QR serve a scansionare i codici QR ed elaborare le informazioni in essi contenute.

Per avviare la scansione del codice QR, toccare e tenere premuta l'icona Sophos e successivamente toccare **Scansione codice QR**.

Indirizzi web

Quando il codice QR viene scannerizzato, l'URL che contiene viene analizzato per rilevare l'eventuale presenza di contenuti malevoli o inappropriati, seguendo la classificazione fornita dai SophosLabs.

- Una volta verificata la sicurezza di un URL, basta toccare **Apri** per aprirlo nel browser web.

Informazioni di contatto

Scansionare il codice QR e procedere come segue:

- Toccare **Aggiungi ai contatti** per creare una voce nei contatti utilizzando le informazioni contenute nel biglietto da visita.
- Toccare **Mostra sulla cartina** per visualizzare la posizione inserita nell'app per le mappe (Google Maps per impostazione predefinita).
- Toccare **Componi numero** per chiamare il numero incorporato. Se il codice QR contiene più di un numero di telefono, le chiamate avverranno nel seguente ordine:
  1. Numero di telefono cellulare
  2. Numero di telefono del lavoro
  3. Numero di telefono di casa
- Toccare **Invia e-mail** per creare una nuova e-mail avente come destinatario l'indirizzo inserito nel codice. Se il codice QR contiene più di un indirizzo e-mail, i destinatari verranno tutti inseriti nel campo **A**.

Additional information
Sophos Intercept X for Mobile è in grado di leggere le informazioni dei biglietti da visita nei formati vCard 2.1 e 3.0.

Configurazioni Wi-Fi

Scansionare il codice QR e toccare **Connetti alla rete** per effettuare la connessione alla rete Wi-Fi configurata nel codice QR.

Nota
Comparirà un avviso che indica che si sta tentando di effettuare la connessione a una rete non protetta, ovvero una rete che non è protetta con WPA o WPA2.

12 App Protection

App Protection serve a configurare un elenco di app che possono essere aperte solamente dopo aver ricevuto l'autorizzazione dell'utente. Ciò è particolarmente utile, nel caso si debba passare il dispositivo ad un altro utente che non potrà, in questo modo, accedere a determinate app.

Nota
Quando Sophos Intercept X for Mobile è gestita da Sophos Mobile, App Protection non è disponibile. L'accesso alle app sarà gestito dall'organizzazione.

1. Nel menù dell'app, selezionare **App Protection**.
2. Sotto **Configurazione di base**, attivare App Protection.
3. L'app Intercept X deve essere amministratore del dispositivo Android. Se questa funzionalità non è ancora stata attivata, si verrà reindirizzati alla pagina pertinente delle **Impostazioni** di Android. Toccare **Attiva**.
4. Selezionare un tipo di autenticazione per **App Protection**.

   Le opzioni disponibili sono **Sequenza**, **PIN**, **Password** e **Impronta digitale** (se il dispositivo è dotato di sensore di impronte digitali).

   Nota
   Quando Sophos Intercept X for Mobile è gestita da Sophos Mobile, l'amministratore può disattivare l'autenticazione tramite impronta digitale.

5. Alcuni programmi di gestione attività possono disabilitare la funzione **App Protection**, terminandone il processo. Per proteggere i gestori delle operazioni è necessario installare l'app Sophos Security & Antivirus Guard. Questa informazione viene specificata in un messaggio all'interno di **Configurazione di base**. Toccare il messaggio per aprire e poi installare l'app in Google Play.
6. Toccare **Periodo di tolleranza** e selezionare la durata di tempo per la quale si desidera memorizzare la password quando si esce da un'app a cui si intende accedere in seguito.
7. **Configurazione della protezione** elenca le app che è possibile utilizzare per disinstallare o disattivare la protezione delle app. È anche possibile proteggere Google Play e altri programmi di installazione, per prevenire l'installazione non monitorata di app sul dispositivo.
8. Passare il dito a sinistra. Viene visualizzata la vista **Selezione app**. Consente di:
   - Selezionare le app presenti nell'elenco **App non protette** per abilitarne la protezione. Le app verranno visualizzate nell'elenco **App protette**.
   - Deselezionare le app presenti nell'elenco **App protette** per disattivarne la protezione. Le app verranno visualizzate nell'elenco **App non protette**.

Sophos Security & Antivirus Guard monitora i processi di **App Protection** e li riavvia all'occorrenza.

Nota
Se non è stato installato Sophos Security & Antivirus Guard, e se rimangono impostazioni di **App Protection**, verrà richiesto di effettuare nuovamente l'installazione. Si consiglia caldamente di effettuare l'installazione.

13 Privacy Advisor

Privacy Advisor mostra i dati relativi alle autorizzazioni di cui sono in possesso le app installate nel dispositivo.

Nota
Questa sezione fornisce una descrizione del Privacy Advisor in Android 6 e versioni successive. Per il Privacy Advisor in Android 5, vedere Privacy Advisor (Android 5) (pagina 20).

Gestione delle autorizzazioni in Android

Le autorizzazioni costituiscono un meccanismo di protezione centrale degli Android, che consente di attribuire diritti specifici a determinate app. Con la versione 6, Android ha modificato il modo in cui le app richiedono le autorizzazioni:

- Le app create per Android 6 o versioni successive richiedono all'utente di concedere le autorizzazioni in runtime, ovvero quando si accede a una funzionalità dell'app che richiede un'autorizzazione che non è ancora stata concessa.
- Le app create per Android 5 o versioni precedenti (dette *app legacy*) richiedono tutte le autorizzazioni necessarie *durante l'installazione*. Quando viene installata un'app legacy su Android 6 e versioni successive, è possibile negare individualmente le singole autorizzazioni. Tuttavia, siccome l'app non è progettata per offrire questa opzione, potrebbe smettere di funzionare.

Le opzioni visibili nel Privacy Advisor

Privacy Advisor mostra lo stato delle autorizzazioni che Google classifica come pericolose, in quanto hanno ripercussioni sulla privacy dell'utente o sul funzionamento di altre app:

- **Autorizzazione calendario** **Calendario**
- **Autorizzazione fotocamera** **Fotocamera**
- **Autorizzazione contatti** **Contatti**
- **Autorizzazione localizzazione** **Posizione**
- **Autorizzazione microfono** **Microfono**
- **Autorizzazione telefono** **Telefono**
- **Autorizzazione sensori del corpo** **Sensori del corpo**
- **Autorizzazione SMS** **SMS**
- **Autorizzazione archiviazione** **Archiviazione**

Un'autorizzazione può avere uno dei seguenti stati:

- **Garantito** Richiesta e concessa
- **Negato** Richiesta e negata

Nota
Per le app legacy, qualsiasi autorizzazione sarà sempre visualizzata come “Richiesta e concessa”, anche se è stata disattivata nelle impostazioni dell'app.

Le azioni disponibili nel Privacy Advisor

- Per visualizzare i dettagli di tutte le autorizzazioni richieste da un'app (incluse le autorizzazioni ritenute non pericolose): toccare l'icona dell'app.
- Per concedere o negare un'autorizzazione: toccare l'icona dell'app e selezionare **Modifica autorizzazioni**, per aprire la pagina dell'app **Informazioni sull'app**. Da questa pagina, toccare **Autorizzazioni**.
- Per visualizzare la cronologia delle modifiche effettuate alle autorizzazioni: toccare **Cronologia delle modifiche delle autorizzazioni** nella barra del titolo.
- Per configurare le opzioni visibili nel Privacy Advisor: toccare **Filtra**. È possibile escludere autorizzazioni o app di un tipo specifico, come ad es. app di sistema o app legacy.
- Per modificare l'ordine delle app: Toccare **Ordina** e selezionare l’ordine in cui devono essere visualizzate le app.

14 Privacy Advisor (Android 5)

Privacy Advisor mostra i dati relativi alle autorizzazioni di cui sono in possesso le app installate nel dispositivo.

Nota
Questa sezione fornisce una descrizione del Privacy Advisor in Android 5. Per il Privacy Advisor in Android 6 e versioni successive, vedere Privacy Advisor (pagina 18).

Sono presenti tre filtri per le autorizzazioni:

- **App che possono incorrere in costi**

  Alcune app possono generare costi aggiuntivi. A seconda delle autorizzazioni richieste dall'app, tale app potrebbe effettuare chiamate a numeri telefonici con tariffe molto elevate, cambiare lo stato della rete del telefono (causando costi aggiuntivi quando il telefono è in roaming), oppure inviare SMS senza richiedere conferma dell'utente.

- **App che possono compromettere la privacy**

  Gli smartphone o tablet contengono informazioni private. Le app a cui vengono assegnate determinate autorizzazioni sono in grado di leggere l'elenco dei contatti. È impossibile controllare come l'app utilizzi le informazioni a cui ha accesso, dal momento che è stata autorizzata ad operare in tal modo. In concomitanza con autorizzazioni specifiche per la connessione, una app potrebbe facilmente inviare tutti i contatti presenti nel dispositivo a terze parti, senza richiedere alcuna conferma. App di questo tipo possono costituire un rischio per la privacy.

- **App che possono accedere a Internet**

  Attualmente, la maggior parte delle app disponibili sul mercato richiedono l'autorizzazione dell'utente per collegarsi a Internet. In concomitanza con altre autorizzazioni, questo potrebbe rappresentare un grave rischio per la sicurezza. È impossibile monitorare informazioni inviate o ricevute da Internet. Verificare quindi se l'accesso a internet è veramente necessario per un'app, e controllare che tale app sia attendibile.

Privacy Advisor presenta l'elenco di tutte le app installate nel dispositivo. Nella parte bassa dello schermo vengono visualizzate le icone relative ai tre filtri del Privacy Advisor. Toccare un'icona per abilitare o disattivare il filtro corrispondente.

I filtri possono essere combinati in modo tale che tutte le app complete delle autorizzazioni compatibili coi filtri selezionati vengano evidenziate.

le app elencate vengono ordinate in base alla relazione fra le autorizzazioni delle app e i filtri selezionati:

- App visualizzate in rosso: le autorizzazioni richieste dalle app indicano un livello di rischio elevato per il filtro selezionato.
- App visualizzate in giallo: le autorizzazioni richieste dalle app indicano un livello di rischio normale per il filtro selezionato.
- App visualizzate in bianco: le autorizzazioni richieste dalle app indicano un livello di rischio basso per il filtro selezionato.

Toccare una voce dell'elenco per visualizzare le informazioni relative a un'app specifica. Il monitor mostra di quali autorizzazioni dispone l'app e in che modo verranno utilizzate.

Se si desidera disinstallare l'app dal dispositivo, toccare **Disinstalla**.

15 Gestione aziendale

In un ambiente aziendale, Sophos Intercept X for Mobile può essere gestita da Sophos Mobile. Questo permette all'organizzazione di monitorare lo stato di conformità del dispositivo.

Per registrare Sophos Intercept X for Mobile a Sophos Mobile, seguire le istruzioni ricevute dalla propria organizzazione.

Quando Sophos Intercept X for Mobile è gestita da Sophos Mobile, sono presenti le seguenti differenze:

- Le impostazioni dell'app verranno definite centralmente dalla propria organizzazione.
- L'organizzazione sarà in grado di avviare scansioni automatiche per determinare lo stato di sicurezza del dispositivo.
- Se il dispositivo non dovesse più rispettare la conformità ai criteri aziendali, l'accesso alla rete o altre funzionalità potrebbero risultare limitati. Lo stato di conformità del dispositivo potrà essere visualizzato nella dashboard dell'app. Vedere Risoluzione delle violazioni della conformità (pagina 21).

Nota
In alternativa, l'organizzazione può gestire il dispositivo, o un'area di lavoro all'interno del dispositivo, con l'app Sophos Mobile Control. Questa opzione concede all'organizzazione un livello di controllo superiore, che include la possibilità di installare o disinstallare app o di disattivare alcune funzionalità del dispositivo. In tale eventualità, sarà possibile visualizzare lo stato di conformità del dispositivo e contattare il personale IT dall'app Sophos Mobile Control. Per informazioni specifiche, consultare la Guida in linea per utenti di Sophos Mobile.

15.1 Risoluzione delle violazioni della conformità

Quando Sophos Intercept X for Mobile è gestita da Sophos Mobile, la dashboard mostra lo stato di conformità in base ai criteri dell'organizzazione.

Per visualizzare e risolvere le violazioni della conformità:

1. Nella dashboard, toccare **Gestione aziendale**.
   In caso di violazioni dei criteri di conformità, il riquadro presenterà un'icona rossa.
2. Toccare la violazione dei criteri di conformità e seguire le istruzioni per risolverla.

Nota
Il mancato rispetto della conformità ai criteri aziendali da parte di un dispositivo potrebbe limitarne l'accesso alla rete o altre funzionalità.

15.2 Supporto

Quando Sophos Intercept X for Mobile è gestita da Sophos Mobile, è possibile visualizzare le modalità di contatto del personale IT ed eventuali altre informazioni fornite.

Nella dashboard, toccare **Gestione aziendale**.

I dettagli del contatto verranno visualizzati sotto **Contatto IT** e **Maggiori info**.

Consiglio
Toccare i campi **E-mail**, **Telefono** o **Dispositivo mobile** per comporre un’e-mail o contattare telefonicamente il personale IT.

16 impostazioni

Impostazione	Descrizione
Scansioni pianificate	Questa opzione effettua scansioni automatiche periodiche.
Intervalli della scansione pianificata	La frequenza con cui vengono effettuate le scansioni pianificate. Se si seleziona **Ogni giorno mentre in carica**, verrà effettuata una scansione quando il dispositivo è connesso a una fonte di alimentazione per più di 30 minuti.
Gestisci app consentite	Toccare questa opzione per visualizzare l'elenco di app consentite. Queste app non compariranno nei risultati delle scansioni. È possibile rimuovere app da questo elenco. Le app rimosse verranno nuovamente visualizzate nell'elenco **Minacce e PUA**.
Cancella predefinite	Toccare questa opzione per non utilizzare più Intercept X come app predefinita per l'apertura dei link supportati.
Scansione delle app di sistema	Selezionare questa opzione per includere nella scansione le app di sistema Android. Le app di sistema non vengono sottoposte a scansione per impostazione predefinita, essendo protette da Android, e non possono essere rimosse dall'utente.
Effettua scansione dell'archiviazione	Selezionare questa opzione per includere nella scansione la scheda SD e i dispositivi di archiviazione USB.
Rileva PUA	Selezionare questa opzione per attivare il rilevamento delle app potenzialmente indesiderate (Potentially Unwanted App, PUA). Le PUA sono app che, sebbene non siano malevole, sono generalmente considerate inadeguate per le reti aziendali. Le PUA sono principalmente classificate come adware, dialer, monitor di sistema, oltre che tool di amministrazione remota e di hacking. Tuttavia alcune delle app che rientrano nella categoria delle PUA, possono essere considerate utili da alcuni utenti.
Reputazione della app	Selezionare questa opzione per attivare il rilevamento delle app con reputazione bassa. Le app con reputazione bassa sono app che hanno ottenuto questo tipo di reputazione in base ai dati raccolti da Sophos Live Protection.

Impostazione	Descrizione
Notifica scansione	Selezionare questa opzione per attivare le notifiche di scansione relative alle app pulite. Deselezionando questa opzione, si riceveranno solamente le notifiche relative a malware, PUA e app con reputazione bassa. Sophos Intercept X for Mobile effettua la scansione delle app durante la loro installazione sui dispositivi Android, oppure in fase di avvio da una scheda SD o un dispositivo di archiviazione USB. Le notifiche si trovano nel Riquadro di notifica.
Monitora l'archiviazione	Attivare questa opzione per effettuare la scansione di tutti i nuovi file e app scaricati o copiati su schede SD o dispositivi di archiviazione USB. Tutti i dispositivi di archiviazione collegati per la prima volta vengono sottoposti a scansione automatica.
Versione	La versione del motore antivirus e dei dati dell'antivirus.
Ultimo aggiornamento	La data in cui i dati dell'antivirus sono stati recuperati da Sophos. Toccare per verificare la disponibilità di aggiornamenti.
Modalità di aggiornamento	Questa impostazione definisce la connessione dati che deve essere utilizzata da Sophos Intercept X for Mobile per scaricare gli aggiornamenti dei dati di rilevamento dei virus.
Invia log per e-mail	Toccare questa opzione per inviare un'e-mail con il file di log dell'app in allegato. Per impostazione predefinita viene inserito l’indirizzo e-mail del Supporto Sophos.
Tracciare i dati per migliorare l'usabilità	Questa impostazione autorizza Sophos a raccogliere dati di utilizzo in maniera anonima, allo scopo di migliorare l'app.
Disinstalla Sophos Intercept X for Mobile	Toccare per disinstallare l'app Intercept X e l'app Security & Antivirus Guard a essa associata, se installata.

17 Backup e ripristino

È possibile eseguire il backup delle impostazioni dell'app, ad esempio per utilizzarle su un altro dispositivo.

L'opzione di backup è disponibile per le seguenti voci:

- Impostazioni
- Scanner
- Filtro web
- App Protection
- Autenticatore

Quando Sophos Intercept X for Mobile è gestita da Sophos Mobile, gli unici backup possibili sono solo quelli degli account Autenticatore.

Effettua backup delle impostazioni

1. Nel menù dell'app, selezionare **Backup e ripristino**.
2. Toccare **Backup**.
3. Selezionare le impostazioni da esportare.
4. Toccare **Backup**.
5. Immettere le credenziali del dispositivo e toccare **Avanti**.
6. Selezionare il percorso in cui creare una copia di backup.

   Consiglio
   Salvare il backup nel proprio spazio di archiviazione nel cloud, in modo tale che possa essere utilizzato su altri dispositivi.

7. Immettere un nome per il file e toccare **Salva**.
8. Immettere una password per la copia di backup, confermarla e toccare **OK**.

Ripristina impostazioni

1. Nella pagina **Backup e ripristino**, toccare **Ripristino**.
2. Aprire il percorso in cui è stato salvato il file e toccare la copia di backup.
3. Immettere la password della copia di backup e toccare **OK**.
4. Selezionare le impostazioni da ripristinare.
5. Toccare **Ripristino**.

18 Registrazione

Sophos Intercept X for Mobile registra nel log le operazioni più importanti. Si tratta di un log diverso dal log di Android. Non si ricevono riscontri immediati sui risultati delle operazioni eseguite in background effettuate dall'app, come ad esempio le scansioni antimalware durante l'installazione di altre app. Il log mette a disposizione report dettagliati su questo tipo di azioni. Indica informazioni dettagliate sull'orario e sui risultati di queste operazioni.

- Per visualizzare il log, toccare **Menu** ≡ e selezionare **Log**.
- Per cancellare il registro, toccare **Elimina** 🗑 nella barra del titolo.

19 Note legali