SOPHOS

Cybersecurity made simple.

Sophos Intercept X for Mobile

Guida in linea (iOS)

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 il lettore di schermo VoiceOver e il software di ingrandimento Zoom, integrato nei dispositivi iOS. I link per l'utilizzo di VoiceOver e di Zoom sono reperibili nelle informazioni correlate. Per ulteriore assistenza con VoiceOver o Zoom, contattare il supporto tecnico di Apple.

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.

Informazioni correlate

Web Content Accessibility Guidelines
Manuale utente di iPhone: Attivare ed esercitarsi con VoiceOver su iPhone
Manuale utente di iPhone: Eseguire lo zoom sullo schermo di iPhone

2 Informazioni su Sophos Intercept X for Mobile

Sophos Intercept X for Mobile aiuta gli utenti a svolgere il proprio lavoro in completa sicurezza su iPhone o iPad.

È possibile aprire un menù di azioni rapide toccando e tenendo premuta l'icona di Sophos. Su un dispositivo 3D Touch basta premere brevemente l'icona per visualizzare il menù.

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

Sotto **Sicurezza dei dispositivi** è possibile visualizzare lo stato di integrità del dispositivo.

Sophos Intercept X for Mobile indica le seguenti informazioni:

- Informazioni generali sul dispositivo, come il nome del modello e la versione di iOS.
- Consigli sull'aggiornamento, se non è installata l'ultima versione di iOS disponibile.
- Informazioni sul jailbreak, se Sophos Intercept X for Mobile ha rilevato jailbreak nel dispositivo.

5 Filtro web

Il Filtro web può essere utilizzato dall'organizzazione per proteggere gli utenti, impedendo loro di accedere a siti web con contenuti malevoli, indesiderati o illegali.

Se il dispositivo è gestito dall'organizzazione, quest'ultima può specificare i tipi di siti web per cui visualizzare un avviso prima dell'apertura e i siti web da bloccare. Questa opzione consente di impedire agli utenti di visitare siti con contenuti malevoli, inappropriati o illegali.

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

Nota

- Questa funzionalità deve essere attivata dall'organizzazione.

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. Scorrere verso il basso alla notifica **Richiesta web bloccata** e toccare **Aggiungi all'elenco Consenti**.

Sotto **Elenco Consenti** viene visualizzato il numero di pagine che sono state autorizzate. Toccare il contatore per visualizzare tutte le pagine.

Le voci aggiunte e quelle predefinite dall'organizzazione vengono visualizzate in sezioni separate.

Per filtrare nuovamente una pagina, far scorrere il dito a sinistra sulla rispettiva voce per eliminarla. Questa azione è disponibile solamente per le voci aggiunte dall'utente stesso.

Elenco Blocca

È possibile aggiungere le pagine web per cui viene generato un avviso a un elenco Blocca, in modo tale che vengano sempre bloccate in futuro. Scorrere verso il basso nella notifica **Richiesta web bloccata** e toccare **Aggiungi all'elenco Blocca**.

Sotto **Elenco Blocca** viene visualizzato il numero di pagine che sono state bloccate. Toccare il contatore per visualizzare le voci di tutte le pagine.

Le voci aggiunte e quelle predefinite dall'organizzazione vengono visualizzate in sezioni separate.

Per filtrare nuovamente un avviso, far scorrere il dito a sinistra sulla rispettiva voce per eliminarla. Questa azione è disponibile solamente per le voci aggiunte dall'utente stesso.

6 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. I tentativi di spoofing dell'ARP non potranno essere rilevati nei dispositivi che eseguono iOS 10.3 o versioni successive.
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.

Nascondere i problemi

È possibile nascondere i problemi del Wi-Fi per reti specifiche. I problemi nascosti non contribuiscono a definire lo stato di integrità del dispositivo.

Per visualizzare nuovamente tutti i problemi, selezionare **Mostra tutti i problemi relativi al Wi-Fi** nelle impostazioni dell'app.

7 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 8).

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 **Toccare per ottenere il codice** per creare il primo codice, oppure **Avanti** per creare il codice successivo. 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, toccarla.
- Per modificare i dettagli dell’account, toccare **Modifica**, selezionare la voce dell’account desiderata e successivamente **Modifica**. Per questioni di sicurezza, non è possibile visualizzare o modificare la chiave segreta.
- Per eliminare un account, toccare **Modifica**, selezionare la voce dell’account desiderata e successivamente toccare l’icona **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.

7.1 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.

7.2 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. Selezionare **Crea > 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.

7.3 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. Selezionare **Crea > 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, immetterle nei campi successivi.

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

   - Nel campo **Periodo di tempo**, inserire il periodo di validità in secondi. Disponibile solamente per password one-time a tempo.
   - 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 **Salva**.

Questa procedura imposterà un nuovo account Autenticatore.

8 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.
- Apri un file KeePass KDBX già esistente. Quando si modificano voci della password, il file originale verrà modificato.

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.

8.1 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 **Più** ⊕.
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.
   - **Note** crea una voce che permette di scrivere una nota protetta.
   - **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 **Più** ⊕ e successivamente **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.

Con **Più** ⊕ è anche possibile aggiungere un file o un'immagine alla voce.

5. Toccare **Fine** 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 11).

Nota
Potrebbero verificarsi problemi di performance in caso di allegati di grandi dimensioni o se è presente un numero elevato di file nella stessa voce. Si consiglia di cifrare questi file con l'app Sophos Secure Workspace per consentirne l'archiviazione sicura.

8.2 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 l'icona **Ingranaggio** 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 **Aggiorna** 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.

8.3 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 l'URL in Safari, toccare l'icona **Globo** accanto al campo **URL**.

8.4 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** .

8.5 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**.

Consiglio
se non si desidera svolgere una ricerca nell'intero file Password Safe, selezionare un gruppo o sottogruppo. Verrà effettuata una ricerca ricorsiva tra tutti gli elementi all'interno del gruppo selezionato.

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

8.6 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. Nel riquadro Password Safe della dashboard dell'app, toccare **Info** ⓘ.
2. Toccare **Effettua backup del file Password Safe**.
3. Selezionare il percorso in cui creare una copia di backup.

Nota
Si consiglia anche di stampare un modulo di recupero che aiuti ad accedere ai dati della password nel caso in cui, ad esempio, si sia dimenticata la password master o si sia smarrito il file di chiave. Vedere Stampa del Modulo di recupero della Password Safe (pagina 12).

8.7 Stampa del Modulo di recupero della Password Safe

Se si dovesse dimenticare la password master di Password Safe o perdere il file di chiave, non sarà possibile accedere ai dati memorizzati in Password Safe. Per evitare questo problema, si consiglia di stampare un modulo di recupero che contiene le informazioni necessarie.

Avviso
È importante effettuare regolarmente backup del file Password Safe. Se si dovesse perdere il file Password Safe, ad esempio in caso di eliminazione non intenzionale del file o smarrimento del dispositivo, il modulo non basterà a recuperare i dati della password. Vedere Backup di Password Safe (pagina 12).

1. Nel riquadro Password Safe della dashboard dell'app, toccare **Info** ⓘ.
2. Toccare **Stampa modulo di recupero**.
3. Selezionare la stampante e il numero di copie desiderate e successivamente toccare **Stampa**.
4. Nel foglio stampato, scrivere le seguenti informazioni:
   - La tua master password
   - La posizione del file Password Safe
   - La posizione della copia di backup
5. Conservare il modulo di recupero in un luogo sicuro.

   Chiunque abbia accesso al modulo di recupero e al file Password Safe potrà leggere i dati della password.

Se il file Password Safe è stato protetto con un file di chiave, un'impronta digitale di questo file sarà inclusa in un codice QR riportato sul modulo di recupero. Questo codice QR potrà essere utilizzato come alternativa al file di chiave per aprire il file Password Safe.

9 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 **Continua** per aprirlo in Safari.

Informazioni di contatto

Scansionare il codice QR e toccare **Aggiungi** per creare una voce nei contatti utilizzando le informazioni contenute nel biglietto da visita.

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 **Copia** per copiare la password negli appunti. Nell'app **Impostazioni**, sotto **Wi-Fi**, selezionare la rete e incollare la password quando viene richiesta.

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.

10 Filtro messaggi

L'organizzazione può utilizzare il Filtro messaggi per individuare eventuali URL di phishing nei messaggi SMS/MMS in entrata.

I messaggi sospetti vengono filtrati sotto un'apposita scheda **SMS indesiderati**.

Se nelle impostazioni dell'app viene visualizzato **Attiva Filtro messaggi**, occorre attivare il filtro dei messaggi nell'app **Impostazioni**, secondo quanto richiesto dall'organizzazione.

Attivazione del Filtro messaggi

Nell'app **Impostazioni** di iOS, selezionare **Messaggi**, toccare **Sconosciuti e spam** e attivare **Intercept X** sotto **Filtro SMS**.

Scheda SMS indesiderati nell'app Messaggi

Se un messaggio proveniente da un mittente sconosciuto viene classificato come spam, il messaggio verrà trasferito nella scheda **SMS indesiderati** dell'app Messaggi. Anche i messaggi esistenti e futuri provenienti dallo stesso mittente verranno trasferiti negli **SMS indesiderati**.

Nota

- I messaggi di un contatto conosciuto non vengono mai classificati come spam.
- Il Filtro messaggi non è compatibile con iMessages.

11 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.
- 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 16).

11.1 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.

11.2 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**.

12 impostazioni

Impostazione	Descrizione
Attiva Filtro messaggi	Individua eventuali URL di phishing nei messaggi SMS/MMS in entrata. Questa funzionalità deve essere attivata dall'organizzazione. Vedere Filtro messaggi (pagina 15).
Attiva Filtro web	Blocca le connessioni alle pagine web malevole o appartenenti a una categoria specifica. Questa funzionalità deve essere attivata dall'organizzazione. Vedere Filtro web (pagina 5).
Mostra tutti i problemi relativi al Wi-Fi	Mostra tutti i problemi relativi al Wi-Fi, inclusi quelli che erano stati precedentemente nascosti.
Livello di log	Se richiesto dal Supporto tecnico Sophos, selezionare il livello di informazioni di log.
Invia file di log	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.
Tracciabilità dei dati	Questa impostazione autorizza Sophos a raccogliere dati di utilizzo in maniera anonima, allo scopo di migliorare l'app.

13 Backup e ripristino

È possibile eseguire il backup degli account Autenticatore per trasferirli su un nuovo dispositivo iOS o Android.

Backup degli account

1. Nel menù dell'app, selezionare **Backup e ripristino**.
2. Toccare **Backup**.
3. Immettere un nome per la copia di backup.
4. Immettere una password, confermarla e toccare **OK**.
5. 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.

6. Toccare **Aggiungi**.

Ripristino degli account

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**.

14 Note legali