SOPHOS

Cybersecurity made simple.

Sophos Secure Workspace

Guida in linea

Versione prodotto: 9.6

Sommario

1 Introduzione

Sophos Secure Workspace consente di archiviare file sui dispositivi mobili oppure nel cloud, anche se si utilizzano vari servizi di archiviazione diversi, garantendo il rispetto della privacy dei dati di natura sensibile. In un ambiente aziendale è possibile voler accedere a documenti e pagine intranet, nonché anche archiviare file, segnalibri e credenziali in un posto sicuro.

Sophos Secure Workspace consente di:

- Visualizzare i documenti archiviati localmente o nel cloud. Vedere Visualizzazione dei documenti (pagina 7).
- Gestire i documenti archiviati localmente o nel cloud. Vedere Gestione dei documenti (pagina 8).
- Annotare documenti e compilare moduli in formato PDF. Vedere Modifica di documenti PDF (pagina 12).
- Prendere appunti. Vedere Creazione di note (pagina 13).
- Scattare foto. Vedere Foto (pagina 14).
- Gestire file di archivio in formato ZIP e 7z. Vedere Gestione dei file di archivio (pagina 16).
- Garantire la privacy dei dati trattati cifrando i documenti che li contengono. Vedere Privacy dei dati trattati (pagina 15).
- Condividere in modo sicuro documenti fra utenti. Vedere Condivisione dei file tra utenti (pagina 16).
- Accedere ai contenuti dei file protetti da password che vengono inviati dagli utenti con SafeGuard Enterprise. Vedere File protetti da password (pagina 22).
- Memorizzare e gestire tutte le password nella Password Safe integrata. Vedere Gestione delle password (pagina 30).

Su iOS 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.

Se si utilizzano altri prodotti Sophos, si potrà disporre di funzionalità aggiuntive.

I clienti che eseguono **Sophos Mobile** possono:

- Creare o modificare file Microsoft Word, Excel o PowerPoint utilizzando l’applicazione integrata Polaris Office. Vedere Modifica di documenti Office (pagina 11).
- Accedere in maniera sicura alle pagine intranet aziendali e ad altre pagine autorizzate. Vedere Accesso all'intranet aziendale (pagina 19).
- Visualizzare in maniera sicura i documenti aziendali. Vedere Visualizzazione dei documenti di lavoro (pagina 21).
- Creare e condividere file protetti da password incapsulati in un formato HTML5. Vedere File protetti da password (pagina 22).
- Gestire le impostazioni di Sophos Secure Workspace e le credenziali dell'archivio in-the-cloud.

I clienti che eseguono **SafeGuard Enterprise** su Windows o macOS possono:

- Condividere in modo sicuro documenti tra dispositivi mobili, notebook e computer desktop. Vedere Condivisione dei file tra dispositivi (pagina 18).
- Utilizzare le chiavi contenute nel proprio keyring SafeGuard. Vedere Gestione delle chiavi (pagina 26).

- Visualizzare le proprie chiavi di ripristino per la cifratura del disco BitLocker e FileVault. Vedere Visualizzazione delle chiavi di ripristino (pagina 29).

Sophos Secure Workspace condivide informazioni con altre app Sophos utilizzando il **contenitore Sophos**:

- La password della app viene utilizzata sia da Sophos Secure Email che da Sophos Secure Workspace.
- Le azioni del contenitore Sophos (blocco, sblocco, reimpostazione della password, annullamento della registrazione) vengono applicate a tutte le app contenitore Sophos.
- I dati e i file possono essere condivisi in maniera sicura tra le app contenitore Sophos.

2 Archiviazione locale

La pagina **Archiviazione locale** mostra i file presenti nel dispositivo.

Su Android, Archiviazione locale contiene i file contenuti nello spazio di archiviazione del dispositivo, scheda SD esclusa.

Su iOS, le app possono accedere solamente ai file situati all'interno del proprio container. Pertanto, Archiviazione locale contiene i file creati o importati in Sophos Secure Workspace.

Copia dei file su un computer

Connettere il dispositivo a un computer Windows o Mac per copiare i file.

(Su Android) Selezionare la modalità USB **Trasferisci file**. Esplora risorse mostra lo spazio di archiviazione del dispositivo, sotto **Questo PC**.

(Su iOS) In iTunes, utilizzare l'elenco **Condivisione file** per Sophos Secure Workspace.

3 Archiviazione sicura

L'Archiviazione sicura è un container sicuro all'interno del dispositivo che è accessibile solo da Sophos Secure Workspace.

Quando nell'Archiviazione sicura si salvano dei file, questi ultimi vengono cifrati con una chiave del dispositivo, a meno che non siano già cifrati.

Quando i file vengono trasferiti all'esterno dell'Archiviazione sicura, saranno decifrati, a meno che non fossero cifrati originariamente.

Sophos Secure Workspace elimina automaticamente i file nell'Archiviazione sicura quando si verificano una o più delle seguenti condizioni:

- L'app Sophos Secure Workspace viene disinstallata.
- L'app Sophos Secure Workspace non è più gestita da Sophos Mobile.
- (Su Android) I dati dell'app vengono eliminati.

4 Connessione dell'archiviazione nel cloud

Per connettere l'account di archiviazione nel cloud a Sophos Secure Workspace:

1. Nella pagina **Home**, procedere in uno dei seguenti modi:
   - (Su Android) Toccare **+**.
   - (Su iOS) Toccare l'icona **Aggiungi archiviazione nel cloud** .
2. Selezionare un provider di archiviazione.
3. Immettere le credenziali.

Sophos Secure Workspace crea un riquadro nella pagina **Home** per ciascun provider di archiviazione connesso.

5 Preferiti

È possibile raccogliere file nell'elenco **Preferiti** per accedervi facilmente. I Preferiti sono disponibili anche quando il dispositivo è off-line.

Per aggiungere un file ai preferiti:

- (Android) Selezionare **Stella** ★ accanto al nome del file.
- (IOS) Selezionare il file e successivamente **Stella** ★.

È anche possibile selezionare una cartella per aggiungere ai preferiti tutti i file contenuti in tale cartella, sottocartelle incluse.

Su Android, i preferiti possono essere aggiunti alla schermata iniziale.

6 Visualizzazione dei documenti

Per visualizzare un documento, aprire e toccare il percorso di archiviazione. Se il file è stato cifrato con una chiave che non è disponibile nel keyring di Sophos Secure Workspace, occorrerà inserire la passphrase relativa alla chiave. I file cifrati sono contrassegnati da un'icona a forma di lucchetto.

Per i tipi di file che possono essere visualizzati e modificati con Sophos Secure Workspace, vedere Provider e formati supportati (pagina 38).

7 Gestione dei documenti

È possibile eseguire varie operazioni sui documenti, come ad esempio la cifratura, il trasferimento su un servizio di archiviazione cloud o la condivisione con altre app.

Operazioni file

È possibile copiare, spostare, rinominare ed eliminare file e cartelle.

Restrizioni:

- Non è possibile copiare o spostare file o cartelle da un servizio di archiviazione cloud a un altro, o all'archiviazione su dispositivo.
- È possibile rinominare solamente un singolo file o cartella alla volta.
- Google Drive non supporta la copia o lo spostamento delle cartelle.
- (iOS) Non è possibile creare cartelle nell'Archiviazione locale.

Visualizzazione delle proprietà del file

È possibile visualizzare proprietà del file quali le dimensioni o i dettagli della chiave di cifratura.

Se Sophos Secure Workspace è gestita da Sophos Mobile, è anche possibile visualizzare informazioni sulle restrizioni per l'utilizzo definite dall'organizzazione.

- (Android) Selezionare un file e successivamente **Dettagli file** dal menù **Operazioni file** .
- (iOS) Selezionare un file e successivamente **Dettagli file** dal menù **Altro** °°°.

Trasferimento di file all'archiviazione cloud

È possibile spostare un file dall'archiviazione su dispositivo all'archiviazione cloud. Il file viene eliminato dal dispositivo.

Nota
Si consiglia di cifrare i file prima di trasferirli nell'archiviazione cloud.

Aggiunta di file ai preferiti

È possibile raccogliere file nell'elenco **Preferiti** per accedervi facilmente. I Preferiti sono disponibili anche quando il dispositivo è off-line.

Per aggiungere un file ai preferiti:

- (Android) Selezionare **Stella** ★ accanto al nome del file.
- (IOS) Selezionare il file e successivamente **Stella** ★.

È anche possibile selezionare una cartella per aggiungere ai preferiti tutti i file contenuti in tale cartella, sottocartelle incluse.

Su Android, i preferiti possono essere aggiunti alla schermata iniziale.

Cifratura e decifratura dei file

È possibile cifrare i file, oppure decifrarli se sono cifrati.

Per cifrare i file:

- (Android) Selezionare i file e successivamente **Cifra**. A seconda delle dimensioni del display, potrebbe essere necessario selezionare prima **Altro**.
- (iOS) Selezionare i file e successivamente **Codifica** dal menù **Altro** °°°.

È inoltre possibile selezionare una cartella per cifrare tutti i file contenuti in tale cartella, sottocartelle incluse.

Per decifrare un file:

- (Android) Selezionare il file e successivamente **Decifra**. A seconda delle dimensioni del display, potrebbe essere necessario selezionare prima **Altro**.
- (iOS) Toccare il file, immettere la passphrase e successivamente selezionare **Decodifica**.

Uso di file provenienti da altre app in Sophos Secure Workspace

È presente l'opzione di utilizzare file provenienti da altre app in Sophos Secure Workspace.

- (Android) Selezionare **+** e successivamente **Importa esistente**.
- (iOS) Selezionare **Importa esistente** dal menù **Altro** °°°.

Se l'opzione è supportata, è anche possibile selezionare i file nell'app di origine e utilizzare **Apri con** (Android) o **Apri in** (iOS) per condividerli con Sophos Secure Workspace.

Nota

- (Android) Quando viene importata una combinazione di file cifrati e non cifrati, non è possibile scegliere di cifrare i file che non sono cifrati. I file vengono importati nel loro stato di cifratura corrente.
- (iOS) È possibile trascinare la selezione per trasferire file tra Sophos Secure Workspace e altre app.
- (iOS) Le attività **Salva in Workspace** e **Visualizza con Workspace** sono disattivate per impostazione predefinita. Per attivarle, toccare **Espandi** nell'elenco **Condividi**.

Uso di file provenienti da Sophos Secure Workspace in altre app

È presente l'opzione di utilizzare file provenienti da Sophos Secure Workspace in altre app. Per svolgere questa operazione, selezionare il file e condividerlo come di consueto.

(Android) Alcune app consentono di selezionare i documenti da Sophos Secure Workspace nelle relative finestre di dialogo di selezione dei file. Ad esempio, in Gmail è possibile selezionare il documento da Sophos Secure Workspace come allegato e-mail.

Nota
Se Sophos Secure Workspace è gestita da Sophos Mobile, la condivisione con alcuni provider di servizi di archiviazione specifici può essere vietata dall'organizzazione.

8 Modifica di documenti Office

Nota
Questa sezione è applicabile solamente se Sophos Secure Workspace è gestita da Sophos Mobile.

Sophos Secure Workspace include una libreria Polaris Office che permette di creare o modificare file Microsoft Word, Excel e PowerPoint.

Creazione di un documento Microsoft Office

Per creare un documento Microsoft Office:

1. Caricare il percorso di archiviazione in cui si desidera creare il nuovo file, e successivamente toccare **+**.
2. Selezionare **Word**, **Excel** o **PowerPoint** per aprire la funzionalità integrata Polaris Office.

Visualizzazione o modifica di documenti Microsoft Office

Per visualizzare o modificare un documento Microsoft Office già esistente:

1. Aprire il percorso dove si trova il file e toccarlo per aprirlo nella funzionalità integrata Polaris Office.
2. Utilizzare il menù di Polaris Office per passare dalla modalità di visualizzazione a quella di modifica e viceversa.

Nota
Quando si modifica un documento Office cifrato, tale documento verrà nuovamente cifrato al momento del suo salvataggio.

Restrizioni

Per i servizi di archiviazione, l'organizzazione ha la possibilità di configurare restrizioni di condivisione. Tali restrizioni hanno i seguenti effetti sulla funzionalità integrata Polaris Office:

- Se l'organizzazione ha negato il permesso di condividere i file, non sarà possibile utilizzare l'opzione **Esporta** in Polaris Office.
- Se l'organizzazione ha negato il permesso di svolgere operazioni con la funzionalità Appunti, l'uso di Polaris Office sarà comunque consentito, ma non sarà possibile copiare e incollare i contenuti degli Appunti in un'altra app.

9 Modifica di documenti PDF

Nota
Questa sezione è applicabile solamente se Sophos Secure Workspace è gestita da Sophos Mobile.

I dispositivi mobili possono essere utilizzati per la revisione di documenti o per l'inserimento di quantità limitate di dati, come quelle richieste durante la compilazione di moduli in formato PDF.

L'app Sophos Secure Workspace è completa di visualizzatore ed editor per documenti PDF integrati.

Per modificare un PDF o compilare un modulo PDF:

1. Aprire il file PDF.
    - Toccare il pulsante **Aggiungi annotazione** per aggiungere annotazioni a un documento. È possibile evidenziare il testo o utilizzare strumenti come note, testo, disegno, linea, rettangolo o freccia.
    - Toccare un campo in un modulo PDF e compilarlo.
2. Salvare le modifiche.

    Se il file era cifrato, viene nuovamente cifrato in maniera automatica al momento del salvataggio.

10 Creazione di note

Sophos Secure Workspace permette di creare una nota rapida. È possibile cifrare la nota per salvaguardare la privacy.

Android:

1. Aprire il percorso di archiviazione in cui si desidera creare il file.
2. Selezionare **+** e successivamente **Testo**.
3. Inserire i propri appunti.
4. Al termine, selezionare **Salva**.
5. Immettere un nome file e selezionare una chiave di cifratura.

iOS:

6. Aprire il percorso di archiviazione in cui si desidera creare il file.
7. Selezionare **Crea > File di testo** dal menù **Altro** °°°.
8. Inserire i propri appunti.
9. Al termine, selezionare **Fine**.
10. Immettere un nome file e selezionare una chiave di cifratura.

Nota
Se Sophos Secure Workspace è gestita da Sophos Mobile, è anche possibile creare o modificare file Microsoft Office. Vedere Modifica di documenti Office (pagina 11).

11 Foto

Sophos Secure Workspace consente di scattare foto e di archiviarle in maniera sicura. Le foto non vengono rese disponibili ad altre app presenti nel dispositivo, a meno che non vengano esplicitamente condivise.

Android:

1. Aprire il percorso di archiviazione in cui si desidera creare la foto.
2. Selezionare **+** e successivamente **Foto** .
3. Scattare la foto.
4. Immettere un nome file e selezionare una chiave di cifratura.

iOS:

5. Aprire il percorso di archiviazione in cui si desidera creare la foto.
6. Selezionare **Crea > Foto** dal menù **Altro** ◦◦◦.
7. Scattare la foto.
8. Immettere un nome file e selezionare una chiave di cifratura.

12 Privacy dei dati trattati

I dati degli utenti sono preziosi e vanno salvaguardati. Si consiglia di cifrare sempre i dati di natura sensibile, sia che siano archiviati in maniera locale che nel cloud.

La cifratura è un metodo che codifica i dati in un formato che risulta leggibile solamente per gli utenti autorizzati. Sebbene la cifratura non impedisca furto o perdita dei dati, è pur sempre in grado di proteggere i dati rendendoli illeggibili e quindi inutilizzabili dagli hacker. Quando si cifra un file, quest'ultimo viene protetto da una chiave, per cui solamente chi conosce questa chiave sarà in grado di accedere al file.

Per una rapida panoramica di come agisce la cifratura in Sophos Secure Workspace, vedere Informazioni relative alla sicurezza (pagina 37).

Cifratura dei file

Sophos Secure Workspace rende la cifratura dei file ancora più semplice.

Quando l'app crea un nuovo file, oppure lo importa da un'altra app, è possibile applicarvi la cifratura.

Per cifrare un file già esistente:

1. Selezionare il file nell'elenco e selezionare l'opzione **Cifra**.
2. Scegliere la chiave di cifratura da utilizzare. Se non è ancora disponibile alcuna chiave, è possibile crearne una.
3. Toccare **OK**. Il file selezionato viene cifrato. Nel caso in cui siano state selezionate cartelle, tutti i file inclusi in tali cartelle verranno sottoposti a cifratura.

Nota
Se si dovesse cifrare un file già cifrato, quest'ultimo verrà ri-cifrato con la nuova chiave. Se dovesse occorrere una passphrase per la vecchia chiave di cifratura, e tale chiave non dovesse essere disponibile nel vostro keyring, verrà richiesto l'inserimento della passphrase.

Nota
Se Sophos Secure Workspace è gestita da Sophos Mobile, sarà possibile cifrare i file solamente con le chiavi incluse nel keyring aziendale, e non con le chiavi locali. Per informazioni sull'uso del keyring aziendale, vedere la sezione Gestione delle chiavi (pagina 26).

Decifratura dei file

Per decifrare file già esistenti, basta selezionarli dall'elenco dei file e quindi selezionare l'opzione **Decifra**.

Sophos Secure Workspace chiede all'utente di inserire la passphrase per poter accedere ai dati. Non verranno richieste passphrase di chiavi già disponibili nel proprio keyring.

Nota
Se Sophos Secure Workspace è gestita da Sophos Mobile, non è possibile decifrare i file.

13 Condivisione dei file tra utenti

Le chiavi di cifratura utilizzate in Sophos Secure Workspace vengono derivate da passphrase.

Non creare una nuova chiave di cifratura per ciascun file, ma pensare invece a come si desidera organizzare l'accesso ai propri contenuti.

Se si dispone di un gruppo di file da condividere con altre persone:

- Cifrare tutti i file utilizzando la stessa chiavi di cifratura.
- Comunicare la passphrase della chiave agli altri utenti.
- Se un altro utente avente accesso allo stesso file (ad es. tramite la condivisione del cloud storage), apre il file dal suo dispositivo, ma la chiave di cifratura necessaria non fa ancora parte del suo keyring, Sophos Secure Workspace richiederà l'inserimento della passphrase. Se questo utente inserisce la passphrase corretta, la relativa chiave di cifratura verrà aggiunta al keyring. Ecco perché è semplicemente necessario distribuire le passphrase e non le chiavi di cifratura.

Nota
due chiavi di cifratura generate dalla stessa passphrase saranno comunque diverse. Ciò è dovuto al fatto che dati casuali vengono aggiunti durante la creazione della chiave per migliorarne il livello di sicurezza. Informare i destinatari dei file cifrati di non creare chiavi di cifratura prima di ricevere i file, ma di attendere che venga richiesto l'inserimento della passphrase per i documenti in questione.

Nota
Se Sophos Secure Workspace è gestita da Sophos Mobile, è possibile condividere i file senza una passphrase se sia il mittente che i destinatari sono in possesso della chiave di cifratura all’interno del keyring aziendale.

13.1 Gestione dei file di archivio

Sophos Secure Workspace consente di gestire file di archivio in formato ZIP e 7z.

Visualizzazione dei contenuti di un file di archivio

È possibile esplorare e visualizzare i contenuti dei file inclusi in un file di archivio in formato ZIP e 7z senza bisogno di estrarli.

- Per esplorare un file di archivio ZIP o 7z, aprire il percorso del file desiderato e toccarlo. Se il file di archivio è protetto da password, occorrerà immettere la password.
- Per visualizzare i contenuti di un file incluso in un file di archivio, aprire il percorso del file desiderato e toccarlo. Se Sophos Secure Workspace supporta il formato del file, tale file si aprirà nel lettore incorporato.

Estrazione di un file di archivio

Per estrarre tutti i file da un file di archivio ZIP o 7z:

- Selezionare il file di archivio e toccare l'opzione **Estrai** nel menù.
- In alternativa, aprire il file di archivio e toccare l'opzione **Estrai tutto** nel menù.

Estrazione di un singolo file da un file di archivio

Per estrarre un singolo file da un file di archivio ZIP o 7z:

1. Aprire il file di archivio.
2. Aprire il percorso del file da estrarre e selezionare il file desiderato.
3. Toccare **Estrai elementi selezionati** nel menù.

Creazione di un file di archivio ZIP

È possibile comprimere i file selezionati e memorizzarli in un nuovo file di archivio ZIP, con l'opzione di applicare la cifratura con password dei file ZIP.

Il file di archivio può anche essere cifrato con una delle chiavi di cifratura del keyring di Sophos Secure Workspace.

Per creare un file di archivio ZIP:

1. Aprire la cartella che contiene i file che si desidera memorizzare in un file di archivio.
2. Selezionare uno o più file e toccare l'opzione **Comprimi** nel menù.

   Non sarà possibile selezionare file dai **Preferiti**, dai **Documenti di lavoro** o dai file **Aperti di recente**.

Nota
Se Sophos Secure Workspace è gestita da Sophos Mobile e se è vietata la condivisione dei file con provider di archiviazione, non sarà possibile memorizzare questi file in un file di archivio.

14 Condivisione dei file tra dispositivi

Nota
Questa sezione è applicabile solamente se Sophos Secure Workspace è gestita da Sophos Mobile.

I file cifrati da Sophos Secure Workspace possono essere letti e modificati da Sophos SafeGuard Enterprise e vice versa.

Sophos SafeGuard Enterprise è una soluzione di classe business per la cifratura del disco e dei file. È disponibile per notebook o workstation desktop con sistema operativo Windows o macOS. I moduli Cloud Storage e File Encryption di SafeGuard Enterprise offrono una soluzione di cifratura dei dati trasparente e basata sul cloud.

Se un file viene condiviso con un dispositivo privo della chiave di cifratura nel keyring, occorrerà inserire la passphrase per aprire il file.

15 Accesso all'intranet aziendale

Nota
Questa sezione è applicabile solamente se Sophos Secure Workspace è gestita da Sophos Mobile.

Browser di lavoro

Il Browser aziendale consente di accedere in maniera sicura alle pagine intranet aziendali e ad altre pagine autorizzate, a seconda delle impostazioni specificate nel criterio di Sophos Mobile. L'organizzazione può definire un set di segnalibri di lavoro a cui è possibile accedere dal browser di lavoro. È poi possibile aggiungere qualsiasi pagina secondaria ai segnalibri personali.

Il browser di lavoro supporta la navigazione a schede, ovvero permette di utilizzare contemporaneamente pagine web multiple. All'avvio del browser di lavoro, verranno riaperte tutte le schede aperte nella sessione precedente.

- Per avviare il browser di lavoro, toccare **Browser di lavoro** nella pagina **Home**.
- Per accedere alle impostazioni dei segnalibri e alle relative funzioni, toccare **Altro** ⋮ nella parte in alto a destra dello schermo (Android), oppure utilizzare la barra degli strumenti (iOS).

Segnalibri

- La pagina **Segnalibri di lavoro** contiene i segnalibri aggiunti dall'organizzazione.
- La pagina **Segnalibri personali** contiene i segnalibri aggiunti dall'utente. Toccare l'icona **Stella** ★ per aggiungere ai segnalibri la pagina web corrente.
- La pagina **Cronologia** contiene un elenco cronologico delle pagine web visitate. Per rimuovere una voce individuale dall'elenco, far scorrere il dito a destra o a sinistra. Per svuotare l'elenco, toccare **Cancella cronologia** (Android) oppure l'icona **Elimina** 🗑 (iOS).

Credenziali

È possibile gestire le credenziali per siti web specifici, se l'organizzazione ha definito il criterio in modo tale da permetterlo.

Quando vengono inseriti nome utente e password, Sophos Secure Workspace chiede se si desidera salvare le proprie credenziali. Toccare **OK** per salvare le credenziali nel gestore credenziali. Saranno disponibili durante la volta successiva che si visita questa pagina.

La pagina **Credenziali** contiene le credenziali salvate. Per eliminare una voce, far scorrere il dito a sinistra o a destra.

Download

La maggior parte dei link contenuti nelle pagine web sono link ad altre pagine. Talvolta può trattarsi di link a documenti o elenchi di file che possono essere gestiti da un'interfaccia web, come ad

esempio SharePoint. Quando si tocca un link a un documento, il browser di lavoro verificherà le autorizzazioni definite per il dominio in questione.

L'organizzazione è in grado di definire le seguenti autorizzazioni:

- Autorizzazione a visualizzare il file.
- Autorizzazione a scaricare e visualizzare il file.
- Autorizzazione a scaricare e aprire il file in un’applicazione diversa.

I file scaricati vengono salvati nell'**Archiviazione sicura**. Se il file non è cifrato, la copia locale verrà cifrata con una chiave del dispositivo.

16 Visualizzazione dei documenti di lavoro

Nota
Questa sezione è applicabile solamente se Sophos Secure Workspace è gestita da Sophos Mobile.

Sophos Mobile include un server di distribuzione dei file indipendente, che viene visualizzato come provider di archiviazione aggiuntivo denominato **Documenti di lavoro**.

La funzionalità Documenti di lavoro può essere utilizzata come segue:

- L'organizzazione può caricare file sul portale web di Sophos Mobile.
- I file sono di sola lettura per gli utenti, i contenuti sono quindi consultabili, ma non modificabili.
- L'organizzazione può definire gruppi di utenti e limitare la visibilità dei file a gruppi specifici.
- L'organizzazione può definire separatamente, per ciascun file, regole per la prevenzione della perdita dei dati. Vedere Impostazioni aziendali (pagina 36).

L'utente viene informato quando sono disponibili documenti nuovi o aggiornati in **Documenti di lavoro**. Ciascun file nuovo o aggiornato viene contrassegnato come nuovo.

Se si contrassegnano come preferiti file o cartelle del provider di archiviazione di **Documenti di lavoro**, Sophos Secure Workspace garantisce la cifratura delle copie off-line con una chiave di cifratura valida esclusivamente per quel dispositivo specifico.

Se l'organizzazione desidera cifrare file da distribuire tramite Sophos Mobile, questa operazione può essere eseguita sia da un dispositivo mobile, cifrando i file presenti nella vista **Archivio locale** di Sophos Secure Workspace, sia (più semplicemente) tramite Sophos SafeGuard Enterprise.

17 File protetti da password

Oltre alla cifratura dei file standard (basata sulle chiavi), Sophos Secure Workspace consente di creare file protetti da password che vengono incapsulati in un formato HTML5, per cui non richiede alcuna installazione di software da parte dei destinatari. Tutto ciò che occorre ai destinatari è la password e un browser web (su Windows oppure macOS), o l'app Sophos Secure Workspace (su Android o iOS) per accedere ai contenuti cifrati.

Ciò è utile ad esempio quando si desidera condividere i file con destinatari esterni all'azienda.

Visualizzazione o modifica dei file protetti da password

È possibile visualizzare i file protetti da password che sono stata creati con Sophos Secure Workspace (su Android o iOS) o SafeGuard Enterprise (su Windows oppure macOS).

Toccare il container HTML e inserire la giusta password per accedere ai contenuti del file.

- Se il container contiene un solo file e se la visualizzazione è supportata per il tipo di file in questione, tale file viene aperto per la visualizzazione. È possibile passare dalla modalità di visualizzazione alla modalità di modifica, se la modifica è supportata per il tipo di file in questione. Quando si salva il file modificato, tale file viene memorizzato come nuovo file all'esterno del container HTML.
- Se il container contiene più di un file, selezionare un percorso di archiviazione in cui memorizzare i file all'esterno del container HTML. Selezionare **Cifra** per cifrare i file nel nuovo percorso. Dopo aver memorizzato i file, è possibile visualizzarli e modificarli.

Creazione di un file protetto da password

Nota
La creazione di file protetti da password è disponibile solamente se Sophos Secure Workspace è gestita da Sophos Mobile.

1. Selezionare il file che si desidera proteggere con password e procedere in uno dei seguenti modi:
   - (Android) Selezionare **Condividi file protetto da password** dal menù **Altro** ⋮.
   - (iOS) Selezionare **Condividi file protetto da password** dal menù **Condividi** ⎙.
2. Inserire una password.
3. Selezionare l'app con la quale si trasferirà il file protetto da password, come ad es. la propria app di posta elettronica.

Nota
Se il file che si desidera condividere è cifrato, Sophos Secure Workspace lo decifrerà, se tale azione è possibile, e successivamente procederà a proteggere con password il file non cifrato.

18 Verifica dei link web nei documenti

Sophos Secure Workspace protegge i sistemi bloccando l’accesso a siti web con contenuti malevoli, indesiderabili o illegali.

- Quando si tocca un link in un documento Microsoft Office o PDF, Sophos Secure Workspace verifica l’URL e visualizza informazioni relative alle minacce della pagina web di destinazione.
- L’accesso alle pagine web non viene bloccato automaticamente. Dopo aver letto le informazioni relative alle minacce, l’utente può decidere se annullare l’operazione oppure aprire la pagina web.
- Le pagine web vengono aperte nel browser di lavoro, se disponibile, oppure nell'app browser predefinita.

19 Password della app

Password della app

È possibile indicare una password per proteggere Sophos Secure Workspace dall'accesso non autorizzato. Se viene attivata questa impostazione, durante il successivo accesso alla app viene richiesto di inserire e confermare la password. La password della app deve essere inserita ogni volta che viene avviato Sophos Secure Workspace.

Si noti che Sophos Secure Workspace utilizza la stessa password di Sophos Secure Email. Eventuali modifiche alla password verranno applicate a entrambe le app. Una volta effettuato l'accesso a una delle app, non occorre inserire le credenziali anche nell'altra app (single sign-on). La password e le configurazioni dell'organizzazione vengono archiviate nel contenitore Sophos, che protegge i dati utilizzati da Sophos nel dispositivo.

L'autenticazione per accedere a Sophos Secure Workspace può essere effettuata mediante impronta digitale. È tuttavia necessario definire una password della app come soluzione alternativa nel caso non fosse possibile leggere l'impronta digitale.

Nota
Su Android, l'autenticazione mediante impronta digitale è disponibile solamente se Sophos Secure Workspace è gestita da Sophos Mobile, e se è supportato dal dispositivo.

Password di ripristino

Sophos Secure Workspace può generare e inviare tramite e-mail una password di ripristino per la password della app. Se ci si dovesse dimenticare la password della app, occorrerà utilizzare tale password di ripristino per creare una nuova password della app. Se ci si dovesse dimenticare la password della app, ma non si disponga della password di ripristino, sarà impossibile utilizzare l'app senza eliminarla e reinstallarla. Quando si elimina l'app, vengono persi tutti i documenti locali gestiti da Sophos Secure Workspace e le chiavi di cifratura contenute nel keyring.

Attenzione
Si consiglia vivamente di creare una password di ripristino. Se si dovesse dimenticare la password della app, sarà possibile effettuarne la reimpostazione solamente con la password di ripristino.

Nota
Se Sophos Secure Workspace è gestita da Sophos Mobile, non occorre impostare una password di ripristino. La password dell'app può essere reimpostata nel portale self-service di Sophos Mobile.

Periodo di tolleranza

Per praticità, è possibile indicare un periodo di tolleranza, ovvero un periodo di tempo entro cui non è necessario inserire nuovamente la password dell'app quando viene avviata. Durante questo periodo di tolleranza, è possibile avviare Sophos Secure Workspace (e Sophos Secure Email) senza dover inserire nuovamente la password. Il periodo di tolleranza è valido solamente quando la app

è nella memoria. Se una app viene caricata dal sistema, occorrerà sempre e comunque inserire la password della app.

Quando un dispositivo è bloccato anche Sophos Secure Workspace viene bloccato, a prescindere dal Periodo di tolleranza impostato.

Imposta password della app

La password dell'app, la password di ripristino e il periodo di tolleranza possono essere impostati nella vista **Impostazioni**.

Cambia la password della app

È possibile cambiare la password della app nella vista **Accesso**, che viene visualizzata quando si avvia Sophos Secure Workspace. Quando si cambia la Password della app, è possibile richiedere una nuova password di ripristino. Nel caso non si richieda una nuova password di ripristino, quella vecchia resterà valida per la nuova password della app.

20 Gestione delle chiavi

Sophos Secure Workspace raccoglie tutte le chiavi di cifratura in gruppi di chiavi. È possibile visualizzarli toccando l'opzione **Chiavi di cifratura** nel menù.

Rimozione del gruppo di chiavi (keyring)

- Quando l'app viene disinstallata, il gruppo di chiavi di Sophos Secure Workspace viene rimosso dal dispositivo.
- I file cifrati situati nel cloud o nelle schede di memoria dei dispositivi Android rimangono cifrati. Una volta rimosso il keyring, non sarà più possibile accedere a questi file.

Smarrimento delle chiavi di cifratura

- In caso di smarrimento della chiave di cifratura, sarà pur sempre possibile accedere ai file cifrati utilizzando la passphrase.
- Sophos Secure Workspace richiederà l'inserimento della passphrase, e procederà quindi ad aggiungere nuovamente la chiave al keyring.

Attenzione
Se si dovesse smarrire la chiave di cifratura e non ci si ricordasse la passphrase, non sarà possibile accedere ai contenuti. non esiste alcuno stratagemma per poter comunque accedere ai contenuti in assenza di chiave di cifratura e passphrase, in quanto un tale accorgimento potrebbe essere sfruttato anche dagli hacker.

Keyring aziendale

Se Sophos Secure Workspace è gestita da Sophos Mobile, l'organizzazione sarà in grado di attivare la sincronizzazione del keyring aziendale con Sophos SafeGuard. Questa operazione fa in modo che le chiavi del keyring di SafeGuard di un utente vengano rese disponibili nel keyring Sophos Secure Workspace.

Ciò significa che:

- Se nel keyring sono presenti chiavi locali nel momento in cui viene attivata la sincronizzazione del keyring aziendale, sarà possibile continuare a utilizzarle.
- Una volta attivata la sincronizzazione con il keyring aziendale, non si potranno creare nuove chiavi locali.
- A seconda della configurazione impostata dall'organizzazione, le chiavi aziendali verranno rimosse dal dispositivo quando viene bloccato il contenitore Sophos, ad esempio quando il dispositivo viola le regole di conformità.

Condivisione delle chiavi di cifratura tramite codici QR

Le chiavi locali possono essere condivise con la massima semplicità, utilizzando codici QR. È ad esempio possibile allegare a un'e-mail la chiave, che i destinatari possono aggiungere al proprio keyring scansionando il codice QR.

Si consiglia di proteggere la chiave esportata con una passphrase. Quando i destinatari aggiungono la chiave al keyring, dovranno immettere la passphrase.

Non è possibile esportare chiavi dal keyring aziendale. È possibile esportare le chiavi locali quando è attivata la sincronizzazione del keyring aziendale, se il criterio aziendale lo consente.

Per esportare una chiave locale:

1. Selezionare la chiave che si desidera esportare e successivamente procedere in uno dei seguenti modi:
   - (Android) Selezionare **Condividi** .
   - (iOS) Selezionare **Esporta**.
2. Immettere una passphrase e selezionare **Proteggi** (Android) o **Condividi con passphrase** (iOS).
3. Quando viene visualizzato il codice QR, selezionare **Condividi** (Android) o **Apri in** (iOS).
4. Allegare la chiave a un'e-mail, oppure selezionare una posizione di archiviazione.

Per importare una chiave:

1. Selezionare **Chiavi di cifratura** nel menù e successivamente procedere in uno dei seguenti modi:
   - (Android) Selezionare l'icona del codice QR e scansionare il codice QR della chiave.
   - (iOS) Selezionare **+** e successivamente **Importa chiave dal codice QR**, e scansionare il codice QR della chiave.
2. Se richiesto, immettere la passphrase.
3. La chiave viene aggiunta al keyring.

21 Visualizzazione dei certificati

Nota
Questa sezione è applicabile solamente se Sophos Secure Workspace è gestita da Sophos Mobile.

È possibile visualizzare i seguenti tipi di certificati:

- Il certificato client di SMC.
- Il certificato client che è stato emesso tramite SCEP, se configurato nel criterio contenitore Sophos.
- Tutti i certificati client e root che sono stati trasferiti sul dispositivo come parte del criterio contenitore Sophos.

Per visualizzare i certificati:

- Toccare **Impostazioni** nel menù, per aprire la vista **Impostazioni**. Nella sezione **Certificati**, i certificati vengono visualizzati con informazioni relative a oggetto e scopo.
- Toccare un certificato per visualizzarne ulteriori informazioni.

22 Visualizzazione delle chiavi di ripristino

Nota
Questa sezione è applicabile solamente se Sophos Secure Workspace è gestita da Sophos Mobile.

In caso di blocco dell'accesso a un computer su cui è attivata la Crittografia unità BitLocker (Windows) o la cifratura completa del disco FileVault (macOS), occorre inserire una chiave di ripristino per sbloccare il computer e poter accedere ai dati.

L'organizzazione può rendere disponibili all'utente le chiavi di ripristino per i computer in Sophos Secure Workspace.

Per visualizzare la chiave di ripristino di un computer:

- Toccare **Chiavi di ripristino** nel menù, per visualizzare un elenco di computer assegnati all'utente. Per i computer Windows, questo elenco contiene voci individuali per ciascuna partizione del disco.
- Toccare una voce dell'elenco per visualizzare la chiave di ripristino per il computer o la partizione del disco selezionata.
- Per sbloccare il computer, seguire le istruzioni visualizzate nella schermata BitLocker (Windows) o FileVault (macOS) del computer.

23 Gestione delle password

Sophos Secure Workspace consente di gestire i file Password Safe KeePass.

Funzioni

- Creazione di un nuovo file Password Safe
- Modifica dei contenuti del file Password Safe
- Copia delle password o di altri dati negli Appunti, per consentirne l'uso in altre app
- Modifica di un file Password Safe KeePass già esistente e situato in un servizio di archiviazione nel cloud

Formati e standard di cifratura supportati

- Sophos Secure Workspace supporta la versione 3 del formato di file KDBX. È in grado di aprire file che utilizzano uno degli algoritmi di cifratura nativi di KeePass (AES, ChaCha20).
- I nuovi file Password Safe vengono creati in formato KDBX versione 3 con cifratura AES.

23.1 Crea file Password Safe

1. Aprire il percorso di archiviazione in cui si desidera creare un file Password Safe.
2. Toccare **+**, e successivamente toccare **Password Safe**.
3. Creare una password master per il file Password Safe. Questa password è richiesta per aprire il file Password Safe.

   Avviso
   Se si dovesse dimenticare la password master, non sarà possibile accedere in alcun modo alle password e ad altri dati presenti nella Password Safe.

4. Richiesto: Per Android, selezionare l'utilizzo di un file di chiave.

   La scelta di utilizzare un file di chiave oltre a una password master aumenta il livello di sicurezza del file Password Safe. Un file di chiave può essere un file a scelta; in alternativa, è anche possibile crearne uno. Deve essere disponibile al momento dell'apertura del file Password Safe.

   Selezionare **Usa file di chiave** e toccare **+** per creare un file; in alternativa, selezionare un file già esistente. Il file di chiave non deve essere memorizzato nello stesso percorso del file Password Safe.

   Avviso
   È necessario effettuare il backup del file di chiave: senza questo file, non sarà possibile aprire il file Password Safe.

   Per iOS, è possibile configurare un file di chiave nelle impostazioni del file Password Safe. Toccare **Modifica password master** e attivare **Usa file di chiave**.

5. Per iOS, immettere le voci richieste nel file Password Safe. Le voci possono essere organizzate in gruppi o sottogruppi.

   Per Android, occorre prima salvare il nuovo file Password Safe e, successivamente, immettere le voci password.
6. Toccare **Crea**, immettere un nome e una posizione e toccare **Archivia**.
7. Richiesto: Selezionare l'opzione che prevede la cifratura del file Password Safe.

   Tutti i file Password Safe vengono cifrati con cifratura dei file KeePass. Quando si seleziona l'opzione di cifratura nella finestra di dialogo **Salva file**, Sophos Secure Workspace aggiunge un ulteriore livello di cifratura alla cifratura KeePass.

Nel percorso specificato viene creato un file KDBX.

23.2 Creazione di una voce Password Safe

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

1. Aprire il file Password Safe e toccare **+**.
2. Selezionare il tipo di voce che si desidera creare:
   - **Account** crea una voce con campi predefiniti che possono essere utilizzati per account web ed elementi simili.
   - **Carta di credito** crea una voce con campi predefiniti che possono essere utilizzati per carte di credito ed elementi simili.
   - **Nota** crea una voce nelle note dello store. Disponibile solo in iOS.
   - **Gruppo** crea una cartella all'interno del file Password Safe per organizzare le voci.
3. Immettere i dati nei campi della voce.
4. Richiesto: Per Android, toccare l'icona accanto al campo **Titolo** per selezionarne uno diverso.
5. Richiesto: Aggiungere campi personalizzati alla voce.
   - (Su Android) Toccare **Aggiungi campo** e successivamente aggiungere un nome e un valore per il campo.
   - (Su iOS) Toccare **+** e selezionare il tipo di campo che si desidera aggiungere.

   Se si attiva **Protetto** per un campo personalizzato, il valore di questo campo sarà nascosto, a meno che non si tocchi sull'icona **Occhio** accanto al campo in questione. Inoltre, i campi protetti sono esclusi dai risultati di ricerca.
6. Una volta terminata l'operazione, salvare la voce:
   - (Su Android) Toccare **Altro**.
   - (Su iOS) Toccare **Fine**.

I dati della password possono essere utilizzati per accedere a una pagina web o a un'app. Vedere Utilizzo dei dati delle password per effettuare l'accesso (pagina 32).

Nota
Su iOS, è possibile allegare file a una voce Password Safe. Tuttavia, potrebbero verificarsi problemi di performance in caso di allegati di grandi dimensioni o se è presente un numero elevato di allegati. Per memorizzare questi file in maniera sicura, si consiglia di effettuarne la cifratura con Sophos Secure Workspace.

23.3 Generazione di password

Sophos Secure Workspace è in grado di generare automaticamente password per conto dell'utente.

1. Nel file Password Safe, aprire la voce per cui si desidera generare una password.
2. Passare alla modalità di modifica:
   - (Su Android) Toccare **Modifica** .
   - (Su iOS) Toccare **Modifica**.
3. Aprire il generatore di password:
   - (Su Android) Toccare **+** accanto al campo della password.
   - (Su iOS) Toccare l'icona **Ingranaggio** .
4. Definire la lunghezza della password e i tipi di carattere che devono essere inclusi nella password.
5. Generare una password secondo le proprie specifiche:
   - (Su Android) Toccare **Genera password**.
   - (Su iOS) Toccare **Aggiorna** .
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.

23.4 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:
  - (Su Android) Toccare l'URL. Se si desidera invece copiare l'URL negli Appunti, toccare e tenere premuto l'URL desiderato.
  - (Su iOS) Toccare l'icona **Globo** accanto al campo **URL**.

Consiglio
In Android, quando si apre una voce, Sophos Secure Workspace aggiunge una notifica all'area di notifica di Android. Da questa notifica è possibile copiare negli appunti i valori di nome utente e password.

23.5 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** : per modificare i contenuti della voce. Disponibile solamente quando è selezionata solo una voce.
   - **Taglia** : per trasferire le voci selezionate in un altro gruppo all'interno del file Password Safe.
   - **Copia** : per copiare le voci selezionate in un altro gruppo all'interno del file Password Safe.
   - **Elimina** : per 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** .

23.6 Ricerca di voci di Password Safe

È possibile cercare nomi di voci e valori dei campi delle voci. In Android vi è anche l'opzione di cercare nomi di gruppi.

1. (Su iOS) 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.
2. Passare alla modalità di ricerca:
   - (Su Android) Toccare **Cerca** .
   - (Su iOS) Scorrere verso il basso nella vista Password Safe.
3. Inserire una stringa di ricerca. L'elenco dei risultati viene aggiornato man mano che si digitano lettere.

> **Nota**
> I campi delle password e i campi configurati come **Protetti** vengono esclusi dai risultati di ricerca.

23.7 Gestione delle password master

Quando in Sophos Secure Workspace viene aperto un file Password Safe protetto con una password master, selezionare **Ricorda password** per memorizzare la password master nel keyring di Sophos Secure Workspace. All'apertura successiva del file Password Safe, non verrà richiesta la password master.

Per visualizzare le password master memorizzate nel keyring di Sophos Secure Workspace, toccare **Password** nel menù.

Per fare in modo che Sophos Secure Workspace dimentichi una password master, eliminarla dal keyring.

24 impostazioni

Impostazione	Descrizione
Attiva gruppo di chiavi	Attivare questa opzione per memorizzare chiavi di cifratura in un keyring. Le chiavi memorizzate nel keyring non richiedono l'immissione di una passphrase.
Attiva password della app	Impostazione di una password per l'apertura dell'app. Si consiglia di selezionare anche l'opzione di creare una password di ripristino. La password di ripristino serve a reimpostare la password dell'app. **Attenzione** Se si dovesse dimenticare la password dell'app, senza una password di ripristino non sarà più possibile utilizzare l'app.
Cambia la password della app	Utilizzare questa opzione per modificare la password dell'app.
Periodo di tolleranza	Selezionare l'intervallo di tempo durante il quale l'app rimarrà sbloccata dopo l'utilizzo.
Blocca screenshot	Abilitare questa opzione per bloccare gli screenshot dell'app.
Nascondi password	Attivare questa opzione per nascondere le password inserite nell'app. Disattivando questa opzione, i caratteri immessi nei campi delle password verranno visualizzati brevemente, prima di essere occultati.
Tracciabilità dei dati	Questa impostazione autorizza Sophos a raccogliere dati di utilizzo in maniera anonima, allo scopo di migliorare l'app.
Invia analisi	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.
Certificati	Visualizza i certificati gestiti da Sophos Mobile. Vedere Visualizzazione dei certificati (pagina 28).

Impostazione	Descrizione
Password della app	Impostazione di una password per l'apertura dell'app. Si consiglia di selezionare anche l'opzione di creare una password di ripristino. La password di ripristino serve a reimpostare la password dell'app. **Attenzione** Se si dovesse dimenticare la password dell'app, senza una password di ripristino non sarà più possibile utilizzare l'app.
Periodo di tolleranza	Selezionare l'intervallo di tempo durante il quale l'app rimarrà sbloccata dopo l'utilizzo.
Autenticazione Touch ID	Attivare questa opzione per abilitare lo sblocco dell'app con la propria impronta digitale.
Nascondi caratteri della password	Attivare questa opzione per nascondere le password inserite nell'app. Disattivando questa opzione, i caratteri immessi nei campi delle password verranno visualizzati brevemente, prima di essere occultati.
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.

25 Impostazioni aziendali

Nota
Questa sezione è applicabile solamente se Sophos Secure Workspace è gestita da Sophos Mobile.

Assegnando un criterio contenitore Sophos al dispositivo dell'utente, l'organizzazione può configurare le impostazioni delle app Sophos Secure Workspace e Sophos Secure Email.

L'organizzazione può:

- Imporre l'utilizzo di password specifiche per le app.
- Definire i requisiti minimi per le passphrase delle app.
- Definire i provider di archiviazione in-the-cloud disponibili.
- Configurare credenziali per l’accesso ai servizi di archiviazione in-the-cloud di WebDAV.
- Configurare credenziali per il provider di archiviazione in-the-cloud Egnyte (iOS).
- Bloccare l'acquisizione di screenshot che mostrano l'app Sophos Secure Workspace o il browser di lavoro (solo Android).
- Limitare l'utilizzo dell'app:
  - Vietare la creazione di preferiti.
  - Vietare le operazioni relative all'utilizzo degli Appunti.
  - Vietare la condivisione di file non cifrati.
  - Vietare la condivisione di file cifrati.
  - Vietare l’accesso a dispositivi che sono stati sottoposti a rooting (Android) o jailbreaking (iOS).
  - Limitare l'utilizzo dell'app a una connessione Wi-Fi specifica.
  - Limitare l'utilizzo dell'app a intervalli di tempo e giorni della settimana specifici (intervallo temporale).
  - Limitare l'utilizzo dell'app a un elenco di luoghi geografici (recinto virtuale).

26 Informazioni relative alla sicurezza

Sicurezza

Archiviazione delle credenziali relative all'archivio in-the-cloud e delle chiavi di cifratura:

- Nei sistemi iOS, vengono utilizzati portachiavi.
- Nei sistemi Android, vengono utilizzati archivi delle chiavi.

Se è stata impostata una password dell’app come descritto in Password della app (pagina 24), vengono cifrati i seguenti dati locali:

- Chiave del dispositivo (utilizzata per archiviazione sicura, dati principali, documenti di lavoro archiviati localmente, download del browser di lavoro)
- Chiavi locali
- Chiavi di cifratura di SafeGuard
- Chiavi di ripristino di BitLocker e FileVault
- Certificati client
- Certificati root
- Criteri contenitore
- Impostazioni di connessione

Avviso
Si consiglia vivamente di creare una password per il blocco dello schermo del dispositivo, al fine di incrementare il livello di protezione del keystore (Android) o keychain (iOS).

Avviso
Si sconsiglia di sottoporre il proprio dispositivo a rooting (Android) o jailbreaking (iOS), in quanto questa operazione indebolisce la sicurezza del keystore o del keychain.

Cifratura di file e chiavi

- Sophos Secure Workspace cifra i file utilizzando lo standard di cifratura AES-256. Ciascun file è dotato di una chiave di cifratura dei dati (data encryption key, DEK) indipendente.
- La DEK è a sua volta cifrata con una chiave di cifratura della chiave (key encryption key, KEK) AES-256 . La DEK cifrata viene archiviata con il file.
- Sophos Secure Workspace calcola la KEK da una passphrase immessa dall’utente, utilizzando lo standard di cifratura PKCS#5.
- È importante ricordare che, date le caratteristiche specifiche di questo metodo e il desiderio di incrementare ulteriormente i livelli di sicurezza, vengono aggiunti alcuni dati casuali, in modo tale che, dalla creazione di due KEK provenienti dalla stessa passphrase, vengano generate due chiavi molto diverse.
- L'elenco delle KEK disponibili per un utente viene denominato "gruppo di chiavi" o "keyring" in Sophos Secure Workspace.

27 Provider e formati supportati

Provider di archivi in-the-cloud supportati

Le soluzioni di archiviazione in the cloud supportate sono:

- Box
- Dropbox e Dropbox Business
- Egnyte
- Google Drive
- Microsoft OneDrive e OneDrive for Business (anche come componente di una sottoscrizione Office 365)
- Telekom MagentaCLOUD (precedentemente Media Center)

Altre soluzioni di cloud storage, quando si adopera Sophos Mobile:

- Tutti i servizi di cloud storage basati su WebDAV (ed es. ownCloud o Strato HiDrive)
- Documenti di lavoro

Formati dei file supportati

Sophos Secure Workspace consente di visualizzare i seguenti tipi di file:

- **Visualizza e modifica:**
  - Documenti PDF: PDF
  - Testo: TXT, TEXT, LOG, ASC, DIFF, CONF, PROPERTIES
  - Microsoft Office (richiede Sophos Mobile): DOCX, XLSX, PPTX
  - File KeePass per Password Safe: KDBX versione 3 con cifratura AES o ChaCha20
  - File archiviati: ZIP (visualizza, estrai, crea)
- **Visualizza solo (con visualizzatore interno):**
  - Immagini: JPG, JPEG, PNG, GIF (non animato), TIFF, TIF, BMP, BMPF, ICO, CUR, XBM
  - Hypertext: HTML, HTM, XHTML
  - Audio (Android): tutti i formati e i codec supportati da Android
  - Audio (iOS): AAC, MP3, M4A, WAV
  - File archiviati: 7z (visualizza, estrai)
- **Visualizza solo (in caso di condivisione con app esterne):**
  - Immagini: JPG, JPEG, PNG, GIF (non animato), TIFF, TIF, BMP, BMPF, ICO, CUR, XBM
  - Hypertext: HTML, HTM, XHTML
  - Documenti: DOC, DOCX, PAGES
  - Fogli di calcolo: XLS, XLSX, CSV, NUMBERS
  - Presentazioni: PPT, PPTX, KEY

- Testo RTF: RTF
- Video: MOV, MP4, M4V

Si prega di notare che le app esterne non sono in grado di decifrare i file cifrati.

Se Sophos Secure Workspace è gestita da Sophos Mobile, è anche possibile visualizzare, modificare e creare file dei seguenti tipi:

- **Visualizzazione (con libreria Polaris Office integrata):**

  I formati di file indicati in corsivo sono supportati solamente nella versione Android.

  - Microsoft Word 97-2013: DOC, DOCX, *DOT*, *DOTX*
  - Microsoft Excel 97-2013: XLS, XLSX, *XLTX*, *CSV*
  - Microsoft PowerPoint 97-2013: PPT, PPTX, *PPS*, *PPSX*, *POT*, *POTX*
- **Modifica (con libreria Polaris Office integrata):**
  - Microsoft Word 97-2013: DOC, DOCX
  - Microsoft Excel 97-2013: XLS, XLSX
  - Microsoft PowerPoint 97-2013: PPT, PPTX
- **Creazione (con libreria Polaris Office integrata):**
  - Microsoft Word 2013: DOCX
  - Microsoft Excel 2013: XLSX
  - Microsoft PowerPoint 2013: PPTX

28 Prodotti Sophos correlati

Se si desidera consultare maggiori informazioni sui prodotti Sophos utilizzare questi link:

- Sophos Mobile: https://www.sophos.com/it-it/products/mobile-control.aspx.
- Sophos SafeGuard Encryption: https://www.sophos.com/it-it/products/safeguard-encryption.aspx.
- Sophos Antivirus and Security per Android: https://play.google.com/store/apps/details?id=com.sophos.smsec&hl=it_IT.

29 Supporto

È possibile ricevere supporto tecnico per i prodotti Sophos in ciascuno dei seguenti modi:

- Visitando la Sophos Community su community.sophos.com/ e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su www.sophos.com/it-it/support.aspx.
- Scaricando la documentazione del prodotto da www.sophos.com/it-it/support/documentation.aspx.
- Aprendo un ticket per il nostro supporto tecnico alla pagina https://secure2.sophos.com/it-it/support/contact-support/support-query.aspx.

30 Note legali