SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise

Guida in linea per utenti

Versione prodotto: 8.3

Sommario

1 Informazioni su SafeGuard Enterprise

Sophos SafeGuard si esegue sugli endpoint Windows per proteggerli. Include diversi moduli.

È possibile che non si disponga di tutte le funzionalità descritte in questa Guida in linea. Questo dipende dalla licenza e dai criteri ricevuti dal responsabile della protezione.

Sophos SafeGuard è configurata e gestita centralmente dal Sophos SafeGuard Management Center.

Per accedere alle informazioni generali della propria installazione di Sophos SafeGuard, cliccare sull'icona di Sophos SafeGuard nella La barra delle applicazioni di Sophos SafeGuard (pagina 7).

Le opzioni più importanti per la cifratura e la decifratura dei file sono disponibili in un menu del tasto destro del mouse di Esplora risorse.

Questo documento è applicabile solamente agli endpoint Windows. Per gli endpoint Mac, consultare la Guida in linea per utenti di SafeGuard Enterprise per Mac.

Moduli:

Cifratura completa del disco

Synchronized Encryption

Cifratura dei file

2 Moduli

2.1 Cifratura completa del disco con BitLocker

La cifratura completa del disco con BitLocker si basa sulla tecnologia Crittografia unità BitLocker inclusa nel sistema operativo. Cifra l'intero hard disk, per cui i dati rimangono protetti anche in caso di furto o smarrimento del computer.

Quando si accede all'endpoint, bisogna immettere le credenziali utente per sbloccare BitLocker. Per ulteriori informazioni, vedere Cifratura di un computer con BitLocker (pagina 10).

Sophos SafeGuard permette di gestire BitLocker sugli endpoint che eseguono uno dei seguenti sistemi operativi:

- Windows 8.1 Professional / Enterprise
- Windows 10 Professional / Enterprise

2.2 SafeGuard File Encryption (in base alle applicazioni)

La cifratura dei file in base alle applicazioni cifra i file creati o modificati con applicazioni specifiche (ad es. Microsoft Word). Un criterio definisce un elenco di applicazioni per le quali viene automaticamente eseguita la cifratura. Questo tipo di cifratura è persistente, per cui il file rimane protetto anche se viene trasferito su un altro percorso, caricato su un servizio di archiviazione nel cloud, oppure inviato tramite e-mail.

Se il responsabile della protezione ha specificato Microsoft Word come applicazione per la quale la cifratura dei file è attiva, qualsiasi file creato e/o salvato con Microsoft Word verrà cifrato con una chiave predefinita. Qualsiasi utente il cui gruppo di chiavi includa questa chiave potrà accedere al file.

- I nuovi file creati con le app o le estensioni dei file specificate saranno cifrati automaticamente.
- Se in possesso della chiave per un determinato file cifrato, sarà possibile leggerlo e modificarne il contenuto.
- Se invece non si possiede la chiave richiesta, non sarà possibile leggerne i contenuti.
- Se si accede a un file cifrato da un computer su cui non è installata File Encryption, non sarà possibile leggerne i contenuti.
- I file che vengono copiati o trasferiti da una cartella non cifrata a una cartella a cui è stata applicata una regola di cifratura verranno cifrati.
- I file che vengono copiati o trasferiti da una cartella cifrata a una cartella non cifrata verranno decifrati.
- I file che vengono copiati o trasferiti da una cartella cifrata a una cartella con una regola di cifratura diversa verranno cifrati in base alla regola della cartella di destinazione.
- Nel caso di file creati da applicazioni per cui File Encryption non è attiva ma alla cui estensione è applicabile una regola di cifratura, verranno cifrati e non potranno essere aperti con l'applicazione che ha creato il file. Un esempio è quando viene creato un file .doc con OpenOffice e OpenOffice non è specificato negli **Elenchi di applicazioni**.

Importante
Se la copia o il trasferimento dei file viene interrotto, ad es. nel caso di un riavvio, l'operazione non sarà ripresa automaticamente. Il risultato potrebbe essere la mancata cifratura di file che dovrebbero invece essere cifrati. Per verificare la corretta cifratura dei file, vedere Cifratura di tutti i file in base al criterio (pagina 12).

Per scoprire quali sono i percorsi del computer in cui i file sono cifrati, vedere Visualizzazione dei percorsi in cui i file sono cifrati (pagina 14).

Per scoprire lo stato di cifratura di uno o più file, cliccare con il tasto destro del mouse sul o sui file e selezionare **SafeGuard File Encryption > Mostra stato di cifratura**.

In Esplora risorse, i file cifrati vengono contrassegnati da un simbolo a forma di lucchetto verde. Se non viene visualizzato un simbolo a forma di lucchetto anche se il file è cifrato, consultare l'articolo 108784 della knowledge base Sophos.

2.3 SafeGuard File Encryption (in base al percorso)

La cifratura dei file in base al percorso permette al responsabile della protezione di definire percorsi in cui i file vengono cifrati automaticamente, ad esempio la cartella **Documenti**.

Una volta assegnato al computer un criterio di **Cifratura File** di tipo **Basata sul percorso**, i file presenti nei percorsi a cui è stato applicato tale criterio vengono cifrati in modo trasparente e senza richiedere alcun intervento da parte dell'utente:

- I nuovi file in un percorso specificato per la cifratura vengono cifrati automaticamente.
- Se in possesso della chiave per un determinato file cifrato, sarà possibile leggerlo e modificarne il contenuto.
- Se invece non si possiede la chiave richiesta, non sarà possibile leggerne i contenuti.
- Se si accede a un file cifrato da un computer su cui non è installata File Encryption, non sarà possibile leggerne i contenuti.

Per scoprire quali sono i percorsi del computer in cui i file sono cifrati, vedere Visualizzazione dei percorsi in cui i file sono cifrati (pagina 14).

Per scoprire lo stato di cifratura di uno o più file, cliccare con il tasto destro del mouse sul o sui file e selezionare **SafeGuard File Encryption > Mostra stato di cifratura**.

In Esplora risorse, i file cifrati vengono contrassegnati da un simbolo a forma di lucchetto verde. Se non viene visualizzato un simbolo a forma di lucchetto anche se il file è cifrato, consultare l'articolo 108784 della knowledge base Sophos.

2.4 SafeGuard Cloud Storage

SafeGuard Cloud Storage offre cifratura in base al percorso dei file memorizzati nel cloud. Non cambia in alcun modo la modalità di utilizzo dei file, ma garantisce che le copie locali dei dati del cloud vengano cifrate in maniera trasparente, e che tali dati rimangano cifrati quando vengono caricati nel cloud.

SafeGuard Cloud Storage rileva automaticamente il provider di servizi di archiviazione nel cloud (se è supportato) e applica il criterio di cifratura alla cartella di sincronizzazione.

SafeGuard Cloud Storage non esegue alcuna cifratura iniziale dei dati. I file memorizzati prima dell'installazione o dell'attivazione tramite criterio di SafeGuard Cloud Storage rimarranno non cifrati.

Se si desidera cifrare questi file, occorrerà prima rimuoverli dal cloud e successivamente aggiungerli di nuovo.

Nota
Non aggiungere file alla cartella di Dropbox rilasciandoli sull'icona di Dropbox presente nel desktop di Windows. Effettuando questa operazione i file verranno infatti copiati in formato testo normale nella cartella di Dropbox. Per accertarsi che i file vengano cifrati, copiarli direttamente nella cartella di Dropbox.

Importante
Quando si decomprime un archivio ZIP utilizzando l'archiver incorporato di Microsoft Windows, tale processo viene bloccato non appena si incontri un file cifrato per cui non si dispone delle chiavi di cifratura. L'utente riceverà un messaggio in cui si informa che l'acceso è stato negato, ma non viene riportata alcuna informazione relativa al fatto che alcuni file non sono stati processati e quindi mancano. Gli altri archivi, per esempio 7-Zip, operano in modo corretto con gli archivi ZIP contenenti file cifrati.

2.5 SafeGuard Data Exchange

SafeGuard Data Exchange offre la cifratura in base al percorso per i file salvati sui supporti di memorizzazione rimovibili, al fine di consentirne la condivisione con altri utenti. Solo gli utenti che dispongono di chiavi valide possono leggere il contenuto dei dati cifrati. Tutti i processi di cifratura e decifratura vengono eseguiti in modo trasparente e richiedono interazione minima da parte dell'utente.

Durante il lavoro quotidiano non si noterà che i dati vengono cifrati. Tuttavia, quando si scollega il supporto rimovibile, i dati restano cifrati e quindi protetti da accessi non autorizzati. Gli utenti non autorizzati possono accedere ai file fisicamente, ma non saranno in grado di leggerli senza SafeGuard Data Exchange e senza disporre della relativa chiave.

Il responsabile della protezione definisce la modalità di gestione dei dati sui supporti rimovibili. Il responsabile della protezione può, ad esempio, stabilire che la cifratura sia obbligatoria per i file memorizzati su tutti i supporti rimovibili. In questo caso tutti i file non cifrati presenti in un supporto vengono inizialmente cifrati. Anche tutti i nuovi file salvati su supporti rimovibili vengono cifrati. Se i file esistenti non devono essere cifrati, il responsabile della protezione può scegliere di consentire l'accesso ai file esistenti non cifrati. In questo caso SafeGuard Data Exchange non eseguirà la cifratura dei file esistenti non cifrati. Tuttavia i nuovi file vengono cifrati. Sarà dunque possibile leggere e modificare i file esistenti non cifrati, ma se rinominati, tali file verranno cifrati. Il responsabile della protezione può inoltre negare l'accesso ai file non cifrati e stabilire che rimangano non cifrati.

Esistono due modi per scambiare file cifrati memorizzati su un supporto rimovibile:

- **SafeGuard Enterprise è installato nel computer del destinatario**: è possibile usare chiavi a disposizione di entrambi gli utenti, oppure creare una nuova chiave. Se si crea una nuova chiave, è necessario fornire al destinatario dei dati la passphrase per utilizzarla.
- **SafeGuard Enterprise *non* è installato nel computer del destinatario:** SafeGuard Enterprise offre SafeGuard Portable. Questa utilità può essere copiata automaticamente sul supporto rimovibile insieme ai file cifrati. Utilizzando SafeGuard Portable e la relativa passphrase, il destinatario può decifrare i file e cifrarli nuovamente senza dover installare SafeGuard Data Exchange nel proprio computer.

Importante
Quando si decomprime un archivio ZIP utilizzando l'archiver incorporato di Microsoft Windows, tale processo viene bloccato non appena si incontri un file cifrato per cui non si dispone delle chiavi di cifratura. L'utente riceverà un messaggio in cui si informa che l'acceso è stato negato, ma non viene riportata alcuna informazione relativa al fatto che alcuni file non sono stati processati e quindi mancano. Gli altri archivi, per esempio 7-Zip, operano in modo corretto con gli archivi ZIP contenenti file cifrati.

2.5.1 Icone sovrapposte

Le icone sovrapposte sono icone di piccole dimensioni visualizzate sopra gli elementi di Windows Explorer. La loro funzione è fornire informazioni rapide sullo stato di cifratura dei file. L'aspetto delle icone dipende dal modulo installato.

Le icone sovrapposte di Data Exchange vengono visualizzate solo sopra file e volumi.

- Il tasto rosso indica che non si dispone della chiave per decifrare il file. Questa icona viene visualizzata solo sopra i file.
- La chiave verde viene sovrapposta ai file cifrati, di cui si dispone della chiave per decifrarli all'interno del proprio gruppo di chiavi. Questa icona viene visualizzata solo sopra i file.
- La chiave grigia viene sovrapposta ai file non cifrati, ma che dispongono di una regola di cifratura. Questa icona viene visualizzata solo sopra i file.
- La chiave gialla viene visualizzata quando un'unità dispone di un criterio di cifratura definito. Questa icona viene visualizzata solo sopra le unità.

Le icone sovrapposte vengono visualizzate solo su volumi non di avvio, supporti rimovibili e CD/DVD. Per quanto riguarda le unità di avvio, le icone sovrapposte vengono visualizzate nella cartella the burning staging (la cartella in cui Windows archivia i file prima di masterizzarli su CD/DVD). Se viene specificata una cartella decifrata, non verrà sovrapposta nessuna chiave grigia sui file decifrati all'interno di tale cartella o delle relative sottocartelle. In linea di massima, se ai file non è applicata alcuna regola di cifratura, non verrà visualizzata nessuna chiave grigia.

Nota
Se non viene visualizzata alcuna icona sovrapposta, consultare l'articolo 108784 della knowledge base Sophos.

2.5.2 Cifratura trasparente

Se le impostazioni definite per il computer specificano che i file sui supporti rimovibili debbano essere cifrati, tutti i processi di cifratura e decifraturavengono eseguiti in modo trasparente.

I file vengono cifrati quando scritti sui supporti rimovibili e decifrati quando copiati o spostati dai supporti rimovibili a un percorso diversa.

I dati vengono decifrati soltanto se vengono copiati o spostati in un percorso a cui non è applicato alcun criterio di cifratura. I dati sono quindi disponibili in questo percorso in formato testo normale. Se al nuovo percorso è applicato un criterio di cifratura diverso, i dati vengono cifrati in base a tale criterio.

2.5.3 Passphrase dei supporti di memorizzazione per i dispositivi rimovibili

SafeGuard Data Exchange consente di definire una passphrase unica per i supporti di memorizzazione, che fornisca accesso a tutti i dispositivi rimovibili connessi al computer. Tale passphrase sarà indipendente dalla chiave utilizzata per la cifratura dei file.

Se specificato, l'accesso ai file cifrati può essere concesso con l'inserimento di un'unica passphrase valida per tutti i supporti. La passphrase del supporto è legata ai computer cui è possibile accedere. Ciò significa che viene utilizzata la stessa passphrase del supporto per tutti i computer.

Per istruzioni sull'impostazione di una passphrase dei supporti di memorizzazione, vedere Utilizzo di una passphrase dei supporti di memorizzazione (pagina 19).

La passphrase del supporto può essere modificata e verrà sincronizzata automaticamente su ciascun computer in uso, non appena vi venga collegato un supporto rimovibile.

La passphrase dei supporti risulta utile nei seguenti scenari:

- Se si desidera utilizzare dati cifrati su supporti rimovibili, in computer in cui non è installato SafeGuard Enterprise (SafeGuard Data Exchange in combinazione con SafeGuard Portable).
- Si desidera scambiare dati con utenti esterni: Fornendo loro la passphrase del supporto, è possibile consentirne l'accesso a tutti i file sul supporto rimovibile con un'unica passphrase indipendentemente dalla chiave utilizzata per la cifratura dei singoli file.

È anche possibile limitare l'accesso a tutti i file fornendo all'utente esterno solo la passphrase di una chiave specifica (una "chiave locale", che può essere creata da un utente SafeGuard Data Exchange). In questo caso l'utente esterno avrà accesso esclusivamente ai file cifrati con questa chiave. Tutti gli altri file risulteranno illeggibili.

Una passphrase dei supporti non è necessaria se si utilizzano le chiavi di gruppo di SafeGuard Enterprise per scambiare dati su supporti rimovibili in un gruppo di lavoro i cui membri condividono tale chiave. In questo caso, se specificato dal responsabile della protezione, l'accesso ai file cifrati su supporti rimovibili è completamente trasparente. Non è necessario inserire alcuna passphrase o password. Questo perché le chiavi di gruppo e le passphrase dei supporti rimovibili possono essere utilizzate contemporaneamente. Poiché il sistema rileva automaticamente una chiave di gruppo disponibile, l'accesso per gli utenti che condividono questa chiave è completamente trasparente. Se non vengono rilevate chiavi di gruppo, viene visualizzata una finestra di dialogo e in cui si richiede di immettere una passphrase del supporto o la passphrase di una chiave locale.

Tipi di supporto supportati

SafeGuard Data Exchange supporta i seguenti tipi di supporti rimovibili:

- Chiave di avvio
- Dischi rigidi esterni collegati tramite USB o FireWire
- Unità CD RW (UDF)
- Unità DVD RW (UDF)
- Schede di memoria nei lettori di schede USB

I Blu-ray Disc e i DVD dual-layer non sono supportati.

3 La barra delle applicazioni di Sophos SafeGuard

Tutte le funzionalità di Sophos SafeGuard sono accessibili dal computer mediante l'icona della barra delle applicazioni di Sophos SafeGuard, situata nella barra delle applicazioni di Windows. La disponibilità di funzioni specifiche dipende dai moduli installati.

Cliccare con il tasto destro del mouse sull'icona della barra delle applicazioni di Sophos SafeGuard per visualizzare le seguenti informazioni:

- **Visualizza**:
  - **Gruppo di chiavi**: Mostra tutte le chiavi disponibili.

    Nota
    Se l'endpoint è stato migrato da un ambiente non gestito a uno gestito, potrebbe essere necessario effettuare un secondo accesso a SafeGuard Enterprise per poter visualizzare le chiavi locali definite dall'utente nel proprio gruppo di chiavi.

  - **Certificato utente**: Mostra le informazioni relative al proprio certificato.
  - **Certificato aziendale**: Mostra le informazioni relative al proprio certificato aziendale.
- **Reimposta credenziali di BitLocker**: Apre una finestra di dialogo che consente di modificare il PIN di BitLocker.
- **Crea nuova chiave**: Apre una finestra di dialogo per la creazione di una nuova chiave da utilizzare per SafeGuard Data Exchange (pagina 4) o SafeGuard Cloud Storage (pagina 3). Disponibile solamente se uno di questi moduli è installato nel computer.
- **Cambia passphrase supporto**: Apre una finestra di dialogo per la modifica della passphrase, vedere SafeGuard Data Exchange (pagina 4).
- **Sincronizza**: Avvia la sincronizzazione con il server di SafeGuard Enterprise. L'avanzamento della sincronizzazione viene indicato dai tooltip. Per avviare la sincronizzazione, è anche possibile fare doppio clic sull'icona della barra delle applicazioni.
- **Stato**: Apre una finestra di dialogo che fornisce informazioni sullo stato corrente del computer protetto da SafeGuard Enterprise:

Campo	Informazioni
Ultimo criterio ricevuto	Data e ora di ricezione dell'ultimo criterio.
Ultima chiave ricevuta	Data e ora di ricezione dell'ultima chiave.
Ultimo certificato ricevuto	Data e ora di ricezione dell'ultimo certificato.
Ultimo contatto server	Data e ora dell'ultimo contatto con il server.

Campo	Informazioni
Stato utente SGN	Stato dell'utente che ha eseguito l'accesso al computer (accesso a Windows): — **in sospeso** La replica dell'utente nella POA di SafeGuard è in sospeso. Ciò significa che la sincronizzazione iniziale dell'utente non è ancora stata completata. Questa informazione è particolarmente importante dopo che si è effettuato il primo accesso a SafeGuard Enterprise, in quanto è possibile accedere mediante Power-on Authentication di SafeGuard soltanto dopo che è stata completata la sincronizzazione dei dati dell'utente. — **Utente SGN** L'utente che ha eseguito l'accesso a Windows è un utente di SafeGuard Enterprise. L'utente SGN può effettuare l'accesso tramite Power-on Authentication; viene quinti aggiunto all'UMA (User Machine Assignment) e riceve un certificato utente e un gruppo di chiavi per accedere ai dati cifrati. — **Utente SGN - proprietario** Presupponendo che le impostazioni predefinite non sono state modificate, un proprietario ha il diritto di abilitare altri utenti ad accedere agli endpoint e diventare utenti SGN. — **Guest SGN** Gli utenti guest di SGN non vengono aggiunti all'UMA, non possono accedere tramite POA, non dispongono di alcun certificato o gruppo di chiavi, ed infine non vengono salvati nel database. — **Guest SGN - account di servizio** L'utente che ha eseguito l'accesso a Windows è un utente guest di SafeGuard Enterprise che ha effettuato l'accesso utilizzando un account di servizio per le attività amministrative. — **Utente di SGN Windows** L'utente Windows di SafeGuard Enterprise non viene aggiunto alla POA di SafeGuard, ma dispone di un gruppo di chiavi per accedere ai file cifrati, come gli utenti di SafeGuard Enterprise. Gli utenti vengono aggiunti all'UMA. Ciò significa che possono effettuare l'accesso a Windows dall'endpoint in uso. — **utente non confermato** Gli utenti non confermati non ottengono accesso al gruppo di chiavi per via di uno dei seguenti motivi: – L'utente ha fornito credenziali errate. – L'utente è un utente locale. – Il server di autenticazione ad AD non è raggiungibile. – Autenticazione non riuscita. – Consultare l'articolo 124328 della knowledge base di Sophos. L'utente deve essere confermato dal responsabile

Campo	Informazioni
Stato del computer SGN	Indica il livello di sicurezza dell'endpoint. — **non applicabile** La funzionalità corrispondente non è attiva. — **Il computer è sicuro** Lo stato di integrità del computer è sicuro. — **Il computer è compromesso** Lo stato di integrità del computer non è sicuro. Di conseguenza le chiavi sono state revocate e non è possibile accedere ai file cifrati.
Stato della cache locale **Pacchetti di dati pronti per essere trasmessi**	Indica se sono presenti pacchetti da inviare al server Sophos SafeGuard.
Stato Local Self Help (LSH) **Abilitato** **Attivo**	Indica se Local Self Help è stato abilitato all'interno di un criterio, e se è stato attivato nel computer dall'utente.
Pronto per la modifica del certificato	Questa dicitura viene visualizzata, se il responsabile della protezione ha assegnato al computer un nuovo certificato per l'accesso con token. È ora possibile modificare il certificato per l'accesso con token. Per ulteriori informazioni, consultare la Guida in linea per utenti di SafeGuard Enterprise.

- **Guida in linea**: Apre la Guida in linea per utenti di SafeGuard Enterprise.
- **Informazioni su SafeGuard Enterprise**: Mostra le informazioni sulla versione corrente di SafeGuard Enterprise.

4 Come effettuare ...

4.1 Cifratura di un computer con BitLocker

A seconda della modalità di accesso impostata dal responsabile della protezione per il computer endpoint in uso, il comportamento del supporto di SafeGuard Enterprise per BitLocker può leggermente differire.

Verrà comunque sempre visualizzata una finestra di dialogo che offre l'opportunità di scegliere se procedere subito alla cifratura o posticiparla.

Se si sceglie di salvare, riavviare e/o cifrare, le operazioni di cifratura non verranno avviate immediatamente. Viene, per prima cosa, effettuato un test dell'hardware per verificare che il computer endpoint risponda a tutti i prerequisiti necessari per portare a termine la cifratura di SafeGuard Enterprise per BitLocker. Il sistema effettua il riavvio e verifica che tutti i requisiti hardware siano rispettati. Se per esempio il TPM o l'unità flash USB non è disponibile o accessibile, verrà richiesto di memorizzare la chiave esterna su un altro dispositivo. Il sistema verifica inoltre se sia possibile fornire le credenziali in modo corretto. Se non si possono fornire le credenziali richieste, il computer viene comunque avviato, ma le operazioni di cifratura non vengono lanciate. Verrà richiesto di inserire nuovamente il PIN o la password. Dopo avere concluso con successo il test hardware, viene avviata la cifratura di BitLocker.

Se si sceglie l'opzione **Rimanda**, la cifratura non verrà avviata e non verrà più chiesto se si desidera effettuare la cifratura del volume in questione fino:

- all'arrivo di un nuovo criterio,
- alla modifica dello stato relativo alla cifratura di BitLocker per un dei volumi, oppure
- al nuovo accesso al sistema.

4.1.1 Salvataggio della chiave di avvio

Se il vostro responsabile della protezione ha specificato **TPM + Chiave di avvio** o **Chiave di avvio** come modalità di accesso, sarà necessario indicare il percorso in cui è stata salvata la Chiave di avvio. Si consiglia di utilizzare un'unità USB flash non cifrata per memorizzare la chiave. Le unità di destinazione valide per salvare le chiavi di avvio vengono elencate nella finestra di dialogo. Successivamente, occorrerà connettere il dispositivo di archiviazione contenente la chiave a ogni avvio del computer.

Selezionare l'unità di destinazione e quindi cliccare su **Salva e riavvia**.

4.1.2 Impostazione della password

Se il responsabile della protezione ha indicato come modalità di accesso **Password**, verrà richiesto di scegliere e confermare una nuova password. Sarà necessario inserire questa password a ogni avvio del computer. La lunghezza e complessità della password dipendono dagli oggetti dei criteri di gruppo specificati dal responsabile della protezione. La specifica finestra di dialogo fornisce informazioni sui requisiti relativi alla password.

Nota
Prestare estrema attenzione durante l'impostazione di un PIN o una password. L'ambiente di preavvio supporta solamente il layout di tastiera EN-US. Se si imposta un PIN o una password con caratteri speciali, potrebbe essere necessario utilizzare tasti diversi quando si effettuerà l'accesso in futuro.

4.1.3 Impostazione del PIN

Se il responsabile della protezione ha indicato come modalità di accesso **TPM + PIN**, verrà richiesto di scegliere e confermare un nuovo PIN. Sarà necessario inserire il PIN a ogni avvio del computer. Lunghezza e complessità vengono definite dagli oggetti criterio di gruppo specificati dal responsabile della protezione. La specifica finestra di dialogo fornisce informazioni sui requisiti relativi al PIN.

Nota
Prestare estrema attenzione durante l'impostazione di un PIN o una password. L'ambiente di preavvio supporta solamente il layout di tastiera EN-US. Se si imposta un PIN o una password con caratteri speciali, potrebbe essere necessario utilizzare tasti diversi quando si effettuerà l'accesso in futuro.

4.1.4 Finestra di dialogo solo TPM

Se il vostro responsabile alla protezione ha scelto **TPM** come modalità di accesso, basterà confermare il riavvio e la cifratura del computer endpoint.

4.2 Reimpostazione di password/PIN dimenticati di BitLocker

Se non dovesse essere possibile accedere al computer per via di un PIN, una password o una chiave USB dimenticata, occorrerà ottenere una chiave di ripristino. Per richiedere una chiave di ripristino:

1. Riavviare il computer e premere il tasto **ESC** nella schermata di accesso di **BitLocker**.
2. Nella schermata **Ripristino BitLocker**, cercare l'**ID chiave di ripristino**.
   L'**ID chiave di ripristino** verrà visualizzato solamente per un breve periodo di tempo. Per visualizzarlo nuovamente, occorre riavviare il computer.
3. Contattare l'amministratore e fornire l'**ID chiave di ripristino**.
   L'amministratore deve individuare la chiave di ripristino del computer nel Sophos SafeGuard Management Center e fornirla all'utente.
4. Nella schermata **Ripristino BitLocker**, immettere la chiave di ripristino.
   È ora possibile riavviare il computer.

Appena effettuato nuovamente l'accesso al sistema, specificare nuove credenziali per BitLocker. A seconda del sistema operativo, viene visualizzata una finestra di dialogo per la reimpostazione delle credenziali. Se la finestra di dialogo non dovesse essere visualizzata automaticamente, cliccare con il tasto destro del mouse sull'icona di Sophos SafeGuard nella barra delle applicazioni, selezionare **Reimposta credenziali di BitLocker** e seguire le istruzioni fornite sullo schermo.

4.3 Reimpostazione di password/PIN dimenticati di BitLocker con Challenge/Response

Procedura Challenge/Response

Per ottenere chiavi di ripristino BitLocker, eseguire la seguente procedura:

1. Riavviare il PC. Una volta riavviato il computer verrà visualizzato un messaggio giallo. Entro tre secondi premere un tasto qualunque della tastiera.
2. Viene visualizzata la schermata di Sophos Challenge/Response.
3. Al Passaggio 2 vengono fornite tutte le informazioni necessarie per contattare l'helpdesk.
4. Fornire le seguenti informazioni all'helpdesk:
   - **Computer**, per esempio Sophos\<nome computer>
   - Codice **Challenge**, per esempio ABC12-3DEF4-56GHO-892UT-Z654K-LM321. Spostare il cursore sui caratteri per visualizzare un correttore ortografico, oppure premere diverse volte il tasto **F1** per far comparire questa casella di assistenza. Il codice scadrà entro 30 minuti con la chiusura automatica del PC.
5. Inserire il **codice Response** dall'helpdesk (sei blocchi con due campi di testo per ogni blocco e cinque caratteri obbligatori per campo).
   - Non appena viene popolato un campo di testo, si passerà automaticamente al campo di testo successivo.
   - Nel caso si inserisca un carattere errato in uno dei due blocchi, il blocco in questione verrà evidenziato in rosso.
6. Una volta inserito il codice Response, cliccare su **Continua** oppure premere **Invio** per concludere la procedura di Challenge/Response.

Reimpostazione delle credenziali BitLocker

Appena effettuato nuovamente l'accesso al sistema, specificare nuove credenziali per BitLocker. A seconda del sistema operativo, viene visualizzata una finestra di dialogo per la reimpostazione delle credenziali. Se la finestra di dialogo non dovesse essere visualizzata automaticamente, cliccare con il tasto destro del mouse sull'icona di Sophos SafeGuard nella barra delle applicazioni, selezionare **Reimposta credenziali di BitLocker** e seguire le istruzioni fornite sullo schermo.

4.4 Cifratura di tutti i file in base al criterio

Una volta assegnato al computer un criterio di **Cifratura file**, i file già presenti nel percorso a cui viene applicato tale criterio di cifratura non verranno cifrati automaticamente. Deve essere eseguita una cifratura iniziale.

Si consiglia di eseguire la cifratura iniziale non appena l'endpoint riceve il criterio di Cifratura file, anche se il responsabile della protezione ha dato inizio alla cifratura automaticamente.

Per avviare manualmente il processo di cifratura, cliccare con il tasto destro del mouse sul nodo **Questo PC** in Esplora risorse e selezionare **SafeGuard File Encryption > Cifra in base al criterio**.

La Procedura guidata di SafeGuard File Encryption (pagina 13) cifra tutti i file presenti nelle cartelle e sottocartelle a cui sono state applicate le regole di cifratura definite.

4.4.1 Procedura guidata di SafeGuard File Encryption

Per aprire la procedura guidata di SafeGuard File Encryption, cliccare con il tasto destro del mouse sul nodo **Questo PC** o su una cartella in Esplora risorse e selezionare **SafeGuard File Encryption > Cifra in base al criterio**.

Verifica tutte le cartelle definite nelle regole di cifratura per utenti:

- I file ordinari da sottoporre a cifratura verranno cifrati utilizzando la chiave definita nella regola.
- I file cifrati e da sottoporre a cifratura utilizzando una chiave differente, verranno nuovamente cifrati con la chiave definita nella regola.
- Se l'utente non possiede la chiave corrente, verrà visualizzato un messaggio d'errore.
- I file cifrati che, secondo quanto previsto dal criterio applicabile, dovrebbero essere in chiaro rimarranno cifrati.

Un'icona indica lo stato dell'operazione in esecuzione:

- **Verde:** l'operazione si è conclusa in modo corretto.
- **Rosso:** l'operazione è stata interrotta da un errore.
- **Giallo:** l'operazione è in esecuzione.

Quattro schede forniscono informazioni dettagliate relative ai file elaborati:

- La scheda **Riepilogo** mostra i contatori relativi ai file individuati o elaborati. Il pulsante **Esporta...** può essere utilizzato per creare report in formato XML in cui vengono elencati i file elaborati e i relativi risultati.
- La scheda **Errori** elenca i file che non sono stati elaborati.
- La scheda **Modificati** mostra i file modificati in modo corretto.
- La scheda **Tutti** elenca tutti i file elaborati ed i relativi risultati.

Se si clicca sul pulsante **Arresta**, nell'angolo in alto a destra, l'operazione viene annullata. Il pulsante **Arresta** viene sostituito dal pulsante **Riavvia** per riavviare l'operazione.

Se viene portata a termine con errori, il pulsante **Arresta** viene sostituito da quello **Riprova**. Se si clicca sul pulsante **Riprova** l'operazione viene avviata di nuovo, ma solo per i file per cui l'operazione non era riuscita.

4.5 Cifratura/decifratura manuale dei file

SafeGuard File Encryption consente di cifrare o decifrare manualmente i singoli file. Cliccare con il tasto destro del mouse su un file e selezionare **Cifratura file di SafeGuard**. Sono disponibili le seguenti funzioni:

- **Mostra stato di cifratura**: Indica se un file sia o meno cifrato, specificando eventualmente la chiave utilizzata.
- **Cifratura in base al criterio**: Vedere Cifratura di tutti i file in base al criterio (pagina 12).
- **Decifratura** (solo per la cifratura dei file in base al percorso): Consente di decifrare un file a cui non è applicata una regola di File Encryption.

- **Decifra il file selezionato** (solo per la cifratura dei file in base alle applicazioni): Consente la decifratura e il salvataggio del file in chiaro. Si consiglia di decifrare il file solamente se non contiene dati di natura sensibile.
- **Cifra il file selezionato** (solo per la cifratura dei file in base alle applicazioni): Consente di cifrare manualmente i file con la chiave specificata nel criterio.
- **Crea file protetto da password**: Questa opzione consente di definire una password per la decifratura manuale dei singoli file e serve a garantire la condivisione sicura dei file con un destinatario che si trova all'esterno della rete aziendale. Vedere Invio di file cifrati tramite e-mail (pagina 15).

Cliccando con il tasto destro del mouse su cartelle o unità, verranno rese disponibili le seguenti funzionalità:

- **Mostra stato di cifratura**: Visualizza un elenco dei file inclusi, con icone che ne indicano lo stato di cifratura e la chiave utilizzata.
- **Cifratura in base al criterio**: Vedere Cifratura di tutti i file in base al criterio (pagina 12).

Le seguenti opzioni sono disponibili solamente per Cloud Storage e Data Exchange:

- **Chiave predefinita**: Mostra la chiave attualmente utilizzata per i nuovi file aggiunti al volume (mediante salvataggio, copia o spostamento). È possibile definire separatamente la chiave standard per ogni singolo volume o supporto rimovibile.
- **Imposta chiave predefinita**: Consente di aprire una finestra di dialogo per la selezione di una chiave predefinita diversa.
- **Crea nuova chiave**: Consente di aprire una finestra di dialogo per la creazione di chiavi locali definite dall'utente.
- **Riattivazione della cifratura**: Il responsabile della protezione può consentire all'utente di decidere se sottoporre a cifratura i file di eventuali supporti rimovibili collegati al proprio computer. Quando si connette un dispositivo rimovibile al computer, viene visualizzato un messaggio in cui si chiede se si desidera eseguire la cifratura dei file presenti nel dispositivo collegato al computer. Il responsabile della protezione può inoltre consentire di memorizzare la scelta fatta per quel determinato supporto. Se si seleziona **Memorizza questa impostazione e non mostrare più questa finestra**, la finestra di dialogo non verrà più visualizzata per il supporto interessato. In questo caso, il nuovo comando **Riattiva la cifratura** comparirà nel menu di scelta rapida del supporto in questione in Esplora risorse di Windows. Selezionare questo comando se si desidera modificare questa impostazione per la cifratura del supporto. Se non si dispone dei diritti adeguati sarà impossibile eseguire questa azione e verrà visualizzato un messaggio di errore. Una volta modificata l'impostazione di cui sopra, verrà chiesto nuovamente di decidere se cifrare il supporto.

4.6 Visualizzazione dei percorsi in cui i file sono cifrati

Se si desidera verificare i percorsi del computer in cui vengono cifrati i file e le chiavi utilizzate per la protezione dei file, è possibile utilizzare lo strumento `FETool` di SafeGuard Enterprise.

Per aprire lo strumento `FETool` di SafeGuard Enterprise, aprire un prompt dei comandi, caricare `C:\Programmi (x86)\Sophos\SafeGuard Enterprise\FileEncryption` e digitare `fetool rli -a`.

Questo comando elenca tutte le regole di cifratura applicate al computer. L'elenco contiene la modalità di cifratura, il percorso completo delle cartelle e le chiavi utilizzate.

4.7 Utilizzo di una password per la protezione di un file

Per inviare e-mail a destinatari che non fanno parte della rete aziendale, si consiglia di cifrare i file e proteggerli con una password. In questo modo i destinatari potranno accedere ai file cifrati senza bisogno che nei loro sistemi sia installato il software SafeGuard Enterprise.

Procedere nel modo seguente:

1. Cliccare con il tasto destro del mouse sul file che si desidera inviare e selezionare **Crea file protetto da password**.
2. Seguire le istruzioni visualizzate sullo schermo e creare una nuova password. Si consiglia di utilizzare una password sicura e di non includerla nella stessa e-mail contenente i file.
   Il file viene cifrato e salvato in formato HTML. Il file HTML può ora essere allegato alle e-mail in completa sicurezza.

   Nota
   - La cifratura richiede spazio libero su disco.
   - Il file HTML cifrato sarà più grande del file originale.
   - La dimensione massima supportata per il file è 50 MB.
   - Per inviare diversi file contemporaneamente, è possibile comprimerli in un file .zip e cifrare il file .zip.

3. Comunicare la password ai destinatari telefonicamente oppure con qualsiasi altro mezzo di comunicazione.
   I destinatari possono utilizzare uno dei seguenti browser per aprire l'allegato protetto da password:
   - Mozilla Firefox
   - Google Chrome
   - Microsoft Internet Explorer 11
   - Microsoft Edge
4. Comunicare ai destinatari che dovranno fare doppio clic sul file e seguire le istruzioni visualizzate sullo schermo per svolgere una delle seguenti operazioni:
   - Immettere la password e cliccare su **Immetti** per accedere al file.
   - Cliccare su **Proteggi un nuovo file con password** per proteggere con password un altro file.

I destinatari possono accedere al file protetto con password. Possono proteggere il file con password quando lo inviano nuovamente al mittente. Possono utilizzare la stessa password o una password diversa. Possono anche scegliere di proteggere con password un nuovo file.

4.8 Invio di file cifrati tramite e-mail

Quando si inviano file cifrati a destinatari all'interno della rete aziendale, non occorre applicare cifratura o decifratura. Se il destinatario è in possesso della giusta chiave, sarà in grado di leggere il file.

Per l'invio di e-mail a destinatari che non fanno parte della rete aziendale, SafeGuard Enterprise offre un add-in di Microsoft Outlook che semplifica il processo di cifratura degli allegati e-mail. Ogni volta che si inviano e-mail con uno o più file in allegato, il sistema richiederà di selezionare la modalità di invio degli allegati. Le opzioni disponibili possono variare a seconda dello stato di cifratura dei file allegati all'e-mail.

Nota
Quando si inviano in allegato elementi incorporati, quali ad es. contatti (.vcf) o e-mail (.msg), non viene visualizzata alcuna richiesta di applicare la cifratura. Vengono inviati in chiaro.

- **Protetti da password**

  Selezionare questa opzione se si inviano file di natura sensibile a destinatari che non appartengono all'azienda.

  Dopo aver definito una password e aver inviato il messaggio, il file viene cifrato e salvato come file HTML. Se la password specificata protegge più di un singolo file, ciascun file viene cifrato separatamente con la stessa password. I file che sono già cifrati vengono decifrati automaticamente prima di essere protetti da password.

  I destinatari potranno aprire il file con il loro browser web non appena verrà loro comunicata la password. Si consiglia di utilizzare una password sicura e di non includerla nella stessa e-mail contenente i file. Si consiglia di comunicare la password ai destinatari telefonicamente oppure con qualsiasi altro mezzo di comunicazione.

  I destinatari possono utilizzare uno dei seguenti browser per aprire l'allegato protetto da password:

  — Mozilla Firefox

  — Google Chrome

  — Microsoft Internet Explorer 11

  — Microsoft Edge

  La decifratura su altri browser, ad es. browser per dispositivi mobili, potrebbe funzionare ma non è supportata attivamente.

  I destinatari possono modificare il file e re-inviarlo utilizzando la stessa password, oppure una nuova. Possono anche scegliere di proteggere con password un nuovo file. Le fasi di questa operazione vengono indicate da una procedura guidata visualizzata nel browser. Per ulteriori informazioni, consultare l'articolo 124440 della knowledge base Sophos.

  È anche disponibile l'opzione di proteggere i file con password in maniera manuale, vedere Utilizzo di una password per la protezione di un file (pagina 15).

- **Non protetto**

  Selezionare questa opzione solamente se l'allegato non contiene alcun dato di natura sensibile. L'invio di allegati e-mail non protetti potrebbe venire inserito nel log e monitorato dal responsabile della sicurezza.

- **Allegati da inviare senza modifica**

  Se l'e-mail contiene allegati che non possono essere protetti da password, è possibile procedere o inviandoli senza alcuna modifica, oppure rimuovendoli dall'e-mail. La finestra di dialogo contiene un elenco di file che non possono essere protetti per uno dei seguenti motivi:

  — Il file è già protetto da password. È possibile decifrare prima il file e utilizzare una nuova password, oppure in alternativa il file può essere inviato senza alcuna modifica, e basterà semplicemente comunicarne la password al destinatario.

— Il file è stato cifrato con una chiave che non è attualmente disponibile nel gruppo di chiavi dell'utente. La chiave potrebbe essere stata temporaneamente revocata per via di un problema di sicurezza, oppure non si possiede la chiave utilizzata per cifrare il file. In tale eventualità, consultare il proprio responsabile della sicurezza.

Quando si invia un'e-mail a destinatari sia interni che esterni, il sistema tratterà l'e-mail come se venisse inviata solamente a domini esterni.

4.9 Creazione di una chiave locale

La chiavi locali possono essere utilizzate per cifrare i file che si trovano in percorsi specifici, su un dispositivo rimovibile o su un servizio di archiviazione nel cloud. Questi percorsi devono essere già stati inclusi in un criterio di cifratura.

Per creare una chiave locale:

1. Cliccare con il tasto destro del mouse sull'icona di Sophos SafeGuard dell'area di notifica nella barra delle applicazioni di Windows, oppure cliccare con il tasto destro del mouse su un volume/ una cartella/un file.
2. Cliccare su **Crea nuova chiave**.
3. Nella finestra di dialogo **Crea chiave**, immettere **Nome** e **Passphrase** della chiave.

   Il nome interno della chiave viene visualizzato nel campo in basso.
4. Confermare la passphrase.

   Se si inserisce una passphrase non sicura, verrà visualizzato un messaggio di avviso. Per aumentare il livello di protezione, si consiglia di utilizzare passphrase complesse. Si può anche decidere di utilizzare una passphrase semplice, nonostante il messaggio di avviso. La passphrase deve inoltre essere conforme ai criteri aziendali. In caso contrario, viene visualizzato un messaggio di avviso.
5. Se si è aperta la finestra di dialogo utilizzando il menu del tasto destro del mouse, verrà ora inclusa la voce **Utilizza come chiave predefinita per il percorso**. Mediante l'opzione **Utilizza come chiave predefinita per il percorso**, è possibile impostare la nuova chiave immediatamente come chiave predefinita per un volume o cartella di sincronizzazione di Cloud Storage.

   La chiave predefinita specificata viene utilizzata per la cifratura durante l'esecuzione di operazioni ordinarie. Tale chiave sarà valida fino a quando non ne verrà impostata un'altra.
6. Cliccare su **OK**.

   La chiave viene creata e diviene disponibile non appena i dati sono sincronizzati con il server SafeGuard Enterprise.

   Se tale chiave viene impostata come predefinita, tutti dati copiati su supporti rimovibili o su una cartella di sincronizzazione di Cloud Storage verranno cifrati utilizzando questa chiave.

Affinché il destinatario possa decifrare tutti i dati presenti sul supporto rimovibile, potrebbe essere necessario cifrare nuovamente i dati sul dispositivo utilizzando la chiave creata localmente. A tale scopo, selezionare **Cifratura file di SafeGuard > Cifra in base al criterio** dal menu di scelta rapida del supporto in Esplora risorse. Selezionare la chiave locale richiesta e cifrare i dati. Se si utilizza una passphrase dei supporti, questa operazione non è necessaria.

4.9.1 Importazione di chiavi da un file

Se si ricevono supporti rimovibili contenenti dati cifrati o si desidera accedere al Cloud Storage localizzato in una cartella condivisa cifrata utilizzando chiavi locali definite dall'utente, è possibile importare nel proprio gruppo di chiavi la chiave necessaria per la decifrazione.

Per importare la chiave, bisogna disporre della relativa passphrase. La passphrase deve essere fornita dall'utente che ha cifrato i dati.

1. Selezionare il file nel supporto rimovibile, e cliccare su **Cifratura file di SafeGuard > Importa chiave da file**.
2. Inserire la passphrase nella finestra di dialogo visualizzata.

La chiave viene importata ed è possibile accedere al file.

4.10 Scambio di dati con SafeGuard Data Exchange

Qui di seguito sono riportati tipici esempi di scambio di dati protetto tramite SafeGuard Data Exchange:

- Scambio di dati con utenti di SafeGuard Enterprise che dispongono di almeno una chiave inclusa nel gruppo di chiavi dell'utente.

  In questo caso, occorre cifrare i dati del supporto rimovibile utilizzando una chiave che sia inclusa anche nel gruppo di chiavi del destinatario (ad esempio nel portatile del destinatario). Il destinatario può utilizzare la chiave per accedere in modo trasparente ai dati cifrati.

- Scambio di dati con utenti di SafeGuard Enterprise che non dispongono delle stesse chiavi dell'utente in questione.

  In questo caso basta creare una chiave locale e cifrare i dati utilizzando tale chiave. Le chiavi create localmente sono protette da una passphrase e possono essere importate in SafeGuard Enterprise. L'utente deve fornire la passphrase al destinatario dei dati. Utilizzando questa passphrase, il destinatario potrà importare la chiave e accedere ai dati.

- Scambio di dati con utenti che non dispongono di SafeGuard Enterprise

  Gli utenti che non hanno SafeGuard Enterprise installata sui propri computer possono utilizzare SafeGuard Portable per accedere ai file cifrati. SafeGuard Portable non è supportata sui Mac. Per maggiori informazioni, consultare:

  — Scambio di dati su supporti rimovibili che non dispongono di SafeGuard Enterprise (pagina 20)

  — Modifica di file con SafeGuard Portable (pagina 24)

4.10.1 Cifratura dei supporti di memorizzazione rimovibili con SafeGuard Data Exchange

La cifratura dei dati non cifrati presenti nei supporti rimovibili ha inizio automaticamente, nel momento in cui i supporti vengono collegati al sistema; in caso contrario, è necessario avviare il processo manualmente. Se si è autorizzati a decidere se cifrare o meno i file presenti nei supporti rimovibili, ogni qual volta venga collegato un supporto rimovibile al proprio computer verrà richiesto il consenso per poter svolgere tale operazione.

Per avviare il processo di cifratura manualmente:

1. Selezionare **SafeGuard File Encryption > Cifra in base al criterio** dal menu del tasto destro del mouse in Esplora risorse. Se non è stata definita una chiave specifica, viene visualizzata una finestra di dialogo per la selezione della chiave.
2. Selezionare una chiave e cliccare su **OK**. Tutti i dati contenuti nei supporti rimovibili vengono cifrati.

La chiave predefinita viene utilizzata nel caso in cui nessun'altra chiave sia stata impostata come predefinita. Se la chiave predefinita viene modificata, la nuova chiave verrà utilizzata per la cifratura iniziale dei supporti rimovibili che si collegheranno ai computer.

Nota
Per lo scambio di dati con altri utenti che dispongono di SafeGuard Enterprise installato nel computer, ma che non utilizzano la stessa chiave dell'utente, sono richieste chiavi locali generate dagli utenti o una passphrase dei supporti di memorizzazione. Queste chiavi sono inoltre richieste per rendere sicuro lo scambio di dati con utenti che non dispongono di SafeGuard Enterprise. È possibile identificare le chiavi locali in base al prefisso (Local_).

Se è selezionata l'opzione **Cifra file in chiaro e aggiorna file cifrati**, i file cifrati con una chiave esistente verranno decifrati e nuovamente cifrati utilizzando la nuova chiave.

Annullamento della cifratura iniziale

Se la cifratura iniziale è configurata in modo da avviarsi automaticamente, si potrebbe avere il diritto di annullarla. In questo caso, il pulsante **Annulla** sarà attivo e verrà visualizzato un pulsante **Avvia**; inoltre, si applicherà un ritardo di 30 secondi all'inizio del processo di cifratura. Se non si seleziona **Annulla** durante questo intervallo di tempo, la cifratura iniziale verrà automaticamente avviata allo scadere dei 30 secondi. Se si clicca su **Avvia**, la cifratura iniziale viene avviata immediatamente.

Cifratura iniziale per utenti con passphrase dei supporti

Se l'utilizzo di una passphrase dei supporti di memorizzazione è stato definito nel criterio, verrà richiesto di immettere la passphrase dei supporti prima della cifratura iniziale. La passphrase dei supporti di memorizzazione è valida per tutti i supporti rimovibili ed è associata al computer o a tutti i computer a cui è possibile accedere.

La cifratura iniziale viene avviata automaticamente non appena inserita la passphrase dei supporti di memorizzazione.

Una volta seguito il primo inserimento della passphrase dei supporti di memorizzazione, la cifratura iniziale verrà automaticamente avviata non appena si connetterà al computer un dispositivo diverso.

La cifratura iniziale non verrà avviata nei computer in cui non è stata impostata una passphrase dei supporti di memorizzazione.

4.10.2 Utilizzo di una passphrase dei supporti di memorizzazione

Se stabilito da un criterio, quando si connette un dispositivo rimovibile per la prima volta dopo l'installazione di SafeGuard Data Exchange, viene richiesto l'inserimento della passphrase dei supporti.

Se viene visualizzata tale finestra di dialogo, specificare la passphrase dei supporti. È possibile utilizzare questa unica passphrase dei supporti per accedere a tutti i file cifrati presenti nei supporti rimovibili, indipendentemente dalla chiave utilizzata per cifrarli.

La passphrase dei supporti è valida per tutti i dispositivi connessi al computer. La passphrase dei supporti può essere utilizzata anche con SafeGuard Portable e consente l'accesso a tutti i file, indipendentemente dalla chiave utilizzata per cifrarli.

Si prega di notare che non è possibile utilizzare una passphrase dei supporti di memorizzazione sui Mac.

Modifica/reimpostazione di una passphrase dei supporti di memorizzazione

È possibile modificare la passphrase dei supporti in qualsiasi momento, utilizzando il comando **Cambia passphrase dei supporto** dal menu dell'icona dell'area di notifica. Viene visualizzata una finestra di dialogo in cui inserire la passphrase vecchia, impostare e confermare quella nuova.

Se non si ricorda la passphrase dei supporti, nella finestra di dialogo è disponibile l'opzione per reimpostarla. Se si seleziona l'opzione **Reimposta passphrase dei supporti** e si clicca su **OK**, viene comunicato che la passphrase dei supporti verrà reimpostata al prossimo accesso.

Disconnettersi immediatamente ed eseguire nuovamente l'accesso. All'utente viene comunicato che non sono presenti passphrase dei supporti nel computer ed è quindi necessario immetterne una nuova.

Sincronizzazione di una passphrase dei supporti di memorizzazione

La passphrase dei supporti presente nei dispositivi e nel computer verrà sincronizzata automaticamente. Se si cambia la passphrase dei supporti di memorizzazione nel computer e si connette un dispositivo in cui è ancora in uso la passphrase precedente, all'utente viene comunicato che le passphrase dei supporti di memorizzazione sono state sincronizzate. Questo vale per tutti i computer a cui è possibile accedere. Si prega di notare che non è possibile utilizzare una passphrase dei supporti di memorizzazione sui Mac.

Dopo aver modificato la passphrase dei supporti, è necessario connettere al computer tutti i supporti rimovibili. In questo modo, la nuova passphrase dei supporti viene immediatamente utilizzata in tutti i dispositivi (sincronizzazione).

4.10.3 Scambio di dati su supporti rimovibili che non dispongono di SafeGuard Enterprise

SafeGuard Portable abilita lo scambio di dati cifrati su supporti rimovibili con destinatari che non sono in possesso di SafeGuard Enterprise.

Nota
SafeGuard Portable non è supportata su computer Mac o su computer in cui è installata Sophos SafeGuard.

I dati cifrati con SafeGuard Data Exchange possono essere cifrati e decifrati utilizzando SafeGuard Portable. L'operazione viene eseguita copiando automaticamente un programma (SGPortable.exe) sui supporti rimovibili.

L'utilizzo di SafeGuard Portable in combinazione con la passphrase dei supporti consente l'accesso a tutti i dati cifrati, indipendentemente dalla chiave locale utilizzata per cifrarli. La passphrase di una chiave locale consente l'accesso unicamente a file che sono stati cifrati usando quella specifica chiave.

I destinatari possono decifrare i dati cifrati e cifrarli nuovamente non appena ricevono l'apposita passphrase dei supporti rimovibili o la passphrase di una chiave locale. Possono utilizzare chiavi esistenti create da SafeGuard Data Exchange, oppure creare una chiave nuova tramite SafeGuard Portable (ad es. per i nuovi file).

Non è necessario che SafeGuard Portable sia installata sui computer dei destinatari. Il programma resta sul supporto rimovibile.

Per ulteriori informazioni, vedere Modifica di file con SafeGuard Portable (pagina 24).

4.10.4 Masterizzazione di file su CD/DVD con SafeGuard Data Exchange

SafeGuard Data Exchange consente di masterizzare file cifrati su CD/DVD utilizzando la Masterizzazione guidata CD di Windows. Il responsabile della protezione deve definire una regola di cifratura per l'unità di registrazione CD. Se per l'unità di registrazione CD non esistono regole di cifratura, i file saranno masterizzati sul CD in formato testo normale.

SafeGuard Disc Burning Extension per la Masterizzazione guidata CD è disponibile solo per la masterizzazione di CD/DVD in formato **Mastered**. Per il Live File System non è necessario utilizzare procedure di registrazione guidata. In questo caso l'unità di registrazione viene utilizzata come qualunque altro supporto rimovibile. Se esiste una regola di cifratura per l'unità di registrazione, i file vengono cifrati automaticamente una volta copiati su CD/DVD.

Nella Masterizzazione guidata CD è possibile specificare il modo in cui i file debbano essere masterizzati sul CD (cifrati o in formato testo normale). Dopo aver inserito il nome del CD, viene visualizzata SafeGuard Removable Disk Burning Extension.

Sotto **Statistica**, vengono visualizzate le seguenti informazioni:

- il numero dei file selezionati per la masterizzazione su CD
- il numero dei file cifrati fra quelli selezionati
- il numero dei file in formato testo normale tra quelli selezionati

Sotto **Stato**, sono visualizzate le chiavi utilizzate per la cifratura dei file cifrati in precedenza.

Per la cifratura dei file da masterizzare su CD viene sempre utilizzata la chiave specificata nella regola di cifratura per l'unità di registrazione dei CD.

Se la regola di cifratura per l'unità di registrazione CD è stata modificata, è possibile che i file da masterizzare sul CD risultino cifrati con chiavi diverse. Se la regola di cifratura è stata disattivata quando sono stati aggiunti i file, è possibile che i file aggiunti siano in formato testo normale nella cartella dei file da copiare sul CD.

Cifratura di file su CD

Per cifrare i file quando li si masterizza su CD, cliccare su **Cifra (nuovamente) tutti i file** .

Se necessario, i file precedentemente cifrati vengono cifrati nuovamente, mentre i file in formato testo normale vengono cifrati per la prima volta. Sul CD i file vengono cifrati utilizzando la chiave specificata nella regola di cifratura per l'unità di registrazione CD.

Masterizzazione di file su CD in formato testo normale

Se si seleziona **Decifra tutti i file**, i file verranno prima decifrati e poi masterizzati sul CD.

Copia di SafeGuard Portable su supporti ottici

Se si seleziona questa opzione, anche SafeGuard Portable verrà copiato su CD. Ciò consente di leggere e modificare file cifrati con SafeGuard Data Exchange senza bisogno di installare SafeGuard Data Exchange.

4.11 Scambio di dati nel cloud con SafeGuard Enterprise

SafeGuard Portable abilita lo scambio di dati cifrati nel cloud con destinatari che non sono in possesso di SafeGuard Enterprise.

SafeGuard Portable consente di accedere ai dati cifrati nel cloud da computer su cui non è installata SafeGuard Enterprise. i dati cifrati con SafeGuard Cloud Storage possono essere cifrati e decifrati utilizzando SafeGuard Portable. L'operazione viene eseguita copiando automaticamente un programma (SGPortable.exe) nella cartella di sincronizzazione.

La passphrase della chiave locale consente l'accesso unicamente a file che sono stati cifrati mediante quella specifica chiave. L'utente in questione o qualsiasi altro destinatario può decifrare i dati cifrati, e cifrarli nuovamente. È necessario comunicare anticipatamente la passphrase della chiave locale al destinatario.

Il destinatario può utilizzare chiavi esistenti, oppure crearne di nuove tramite SafeGuard Portable (ad esempio per nuovi file).

Non è necessario installare o copiare SafeGuard Portable nel computer della persona con cui si stanno scambiando i dati. Resta infatti nell'archvio in the cloud.

Per una descrizione dettagliata di come utilizzare SafeGuard Portable, vedere Modifica di file con SafeGuard Portable (pagina 24).

Un doppio clic su un file o la selezione del comando "Apri" non avviano la decifratura istantanea del file. Questo è dovuto al fatto che i file decifrati nelle cartelle di sincronizzazione del servizio di archiviazione nel cloud vengono automaticamente sincronizzati con il cloud. Quando si esegue questa operazione, viene visualizzata una finestra di dialogo in cui si richiede di scegliere un percorso sicuro in cui posizionare il file. I file decifrati non vengono eliminati automaticamente alla chiusura di SafeGuard Portable. I cambiamenti apportati ai file decifrati utilizzando SafeGuard Portable per Cloud Storage non vengono applicati agli originali cifrati.

Nota
Non memorizzare cartelle di sincronizzazione per l'archiviazione in the cloud su supporti rimovibili o nella rete. Se lo si fa, SafeGuard Portable creerà file non cifrati in quelle cartelle.

4.12 Uso di chiavi predefinite

Definendo una chiave predefinita, si specifica la chiave da utilizzare per la cifratura durante l'esecuzione di operazioni ordinarie da parte di SafeGuard Data Exchange e SafeGuard Cloud Storage.

Il responsabile della protezione deve autorizzare esplicitamente l'utilizzo di chiavi predefinite per Cloud Storage. Se viene fornita l'autorizzazione, sarà possibile scegliere una chiave da un gruppo di chiavi predefinite e utilizzarla per cifrare le cartelle nel cloud.

La chiave predefinita può essere impostata dal menu di scelta rapida nei seguenti percorsi:

- supporti rimovibili
- file su supporti rimovibili
- cartelle o sottocartelle di sincronizzazione di Cloud Storage

- file in una cartella o sottocartella di sincronizzazione di Cloud Storage
- Inoltre, è anche possibile impostare immediatamente una nuova chiave come chiave predefinita durante la creazione di una nuova chiave locale nella finestra di dialogo **Crea chiave**.

Per definire una chiave predefinita, selezionare **SafeGuard File Encryption > Imposta chiave predefinita**.

La chiave selezionata in questa finestra di dialogo viene utilizzata per tutti i successivi processi di cifratura; sia per quelli eseguiti su tale supporto di archiviazione rimovibile, sia per quelli eseguiti nella cartella di sincronizzazione di Cloud Storage. Se si desidera utilizzare una chiave diversa, è possibile impostare una nuova chiave predefinita in qualsiasi momento.

Se per la cifratura di Cloud Storage è stata scelta una chiave locale, SafeGuard Portable verrà copiata nella cartella di sincronizzazione di Cloud Storage.

Se si desidera leggere file cifrati su dispositivi Android e iOS utilizzando Sophos Secure Workspace, occorrerà utilizzare chiavi locali per la cifratura. Per ulteriori informazioni, consultare la Guida in linea per utenti di Sophos Secure Workspace.

Esempio

Si desidera utilizzare Dropbox per rendere disponibili dati protetti a collaboratori multipli e si desidera che ciascun collaboratore possa accedere solamente a una sottocartella. Per fare ciò, basta semplicemente impostare una chiave predefinita diversa per ciascuna sottocartella. SafeGuard Enterprise aggiungerà automaticamente a ogni sottocartella una copia di SafeGuard Portable, che consente di accedere ai dati cifrati anche ai collaboratori che non dispongono di SafeGuard Cloud Storage. Si dovrà quindi comunicare ai collaboratori le passphrase abbinate a ciascuna chiave. Utilizzando SafeGuard Portable e la passphrase a disposizione, ciascun collaboratore potrà decifrare i dati contenuti nella cartella creata per lui, ma non avrà accesso ai dati memorizzati nelle altre cartelle, essendo esse cifrate con chiavi diverse.

4.13 Ripristino di file cifrati

Se un file è cifrato con una chiave che non è disponibile nel proprio gruppo di chiavi, sarà impossibile aprire tale file. Ciò potrebbe essere dovuto al fatto che non si possiede l'autorizzazione di accedere a questo file, secondo quanto specificato nel criterio aziendale. Tuttavia, in alcuni casi può capitare di avere diritto di accedere al file, ma di non poterlo visualizzare poiché non si dispone della giusta chiave. In tale eventualità occorre scoprire quale sia la chiave utilizzata e chiedere al responsabile della protezione di assegnare tale chiave al proprio gruppo di chiavi. Procedere come di seguito:

1. Cliccare con il tasto desto del mouse sul file, e successivamente selezionare **Cifratura file di SafeGuard > Mostra stato di cifratura**.
   Verrà visualizzata la chiave utilizzata per cifrare il file selezionato.
2. Contattare il proprio responsabile della protezione, comunicando il nome della chiave.
3. Chiedere al responsabile della protezione di assegnare la chiave al proprio gruppo di chiavi.
4. Non appena il responsabile della protezione conferma l’avvenuto aggiornamento del criterio utente, cliccare con il tasto destro del mouse sull’icona di Sophos SafeGuard visualizzata nell'area di notifica della barra delle applicazioni del computer.
5. Cliccare su **Sincronizza**.
6. Cliccare nuovamente con il tasto destro del mouse sull'icona nell'area di notifica, e successivamente cliccare su **Stato**.
   Verrà visualizzata una finestra di dialogo che indica la data in cui l’ultima chiave è stata trasferita sul computer. Verrà visualizzata la data odierna sotto **Ultima chiave ricevuta**, una volta che la chiave richiesta è stata aggiunta al proprio gruppo di chiavi.

Sarà ora possibile accedere al file.

4.14 Verifica della connessione al server di SafeGuard Enterprise

Se si dovessero riscontrare difficoltà durante la sincronizzazione del proprio endpoint con il server, è possibile utilizzare lo strumento di Verifica della connettività tra client e server per scoprire perché non è possibile stabilire una comunicazione tra l'endpoint e il server di SafeGuard Enterprise.

Per aprire lo strumento di Verifica della connettività tra client e server di SafeGuard Enterprise, navigare su `C:\Programmi (x86)\Sophos\SafeGuard Enterprise\Client` ed eseguire l'applicazione `SGNCSCC.exe`.

Per ulteriori informazioni, consultare l'articolo 109662 della knowledge base Sophos.

4.15 Modifica di file con SafeGuard Portable

Se si è utenti di Sophos SafeGuard, non è necessario utilizzare SafeGuard Portable. La seguente descrizione riguarda gli utenti che non dispongono di Sophos SafeGuard installata nel computer e che devono quindi utilizzare SafeGuard Portable per modificare i dati cifrati.

L'utente riceve file cifrati con SafeGuard Data Exchange, accompagnati da una cartella denominata `SGPortable`. Questa cartella contiene il file `SGPortable.exe`.

1. Avviare SafeGuard Portable cliccando due volte su `SGPortable.exe`.

   Utilizzando SafeGuard Portable è possibile decifrare e cifrare nuovamente i dati cifrati.

   Oltre ai dettagli del file, SafeGuard Portable contiene anche la colonna **Chiave**. Questa colonna indica se i dati sono cifrati o meno. Se un file è cifrato, viene visualizzato il nome della chiave utilizzata. È possibile decifrare i file soltanto se si è a conoscenza della passphrase per la chiave utilizzata.
2. Per modificare un file, fare doppio clic sul file desiderato e selezionare uno dei seguenti comandi:

Imposta chiave di cifratura	Apre la finestra di dialogo **Inserisci chiave**. In questa finestra è possibile generare una chiave di cifratura tramite SafeGuard Portable.
Cifra	Cifra il file con l'ultima chiave utilizzata.
Decifra	Apre la finestra di dialogo **Inserisci passphrase** per consentire l'immissione della passphrase di decifratura del file selezionato.
Stato della cifratura	Visualizza lo stato di cifratura di un file.
Copia in	Consente di copiare il file in una cartella di propria scelta e di decifrarlo.
Elimina	Elimina gli elementi selezionati.

   È anche possibile selezionare i comandi **Apri**,**Elimina**, **Cifra**, **Decifra** e **Copia** utilizzando le icone presenti nella barra degli strumenti.

4.15.1 Impostazione di chiavi di cifratura per SafeGuard Portable

Per impostare una chiave di cifratura per SafeGuard Portable:

1. Dal menu di scelta rapida o dal menu **File**, selezionare **Imposta chiave di cifratura**.

   Viene visualizzata la finestra di dialogo **Inserisci chiave**.
2. Inserire un **Nome** e una **Passphrase** per la chiave.
3. Confermare la passphrase e cliccare su **OK**.

   La passphrase deve essere conforme ai criteri aziendali. In caso contrario, viene visualizzato un messaggio di avviso.

La chiave verrà creata e utilizzata per la cifratura.

4.15.2 Cifratura di file con SafeGuard Portable

1. In SafeGuard Portable, cliccare con il tasto destro del mouse sul file e selezionare **Cifra**.

   Il file viene cifrato con l'ultima chiave utilizzata da SafeGuard Portable.

   Quando si salvano file mediante trascinamento della selezione, viene richiesto se si desidera cifrarli.

   Se non è stata impostata una chiave predefinita, si apre una finestra di dialogo che consente di impostarne una. Immettere il nome della chiave e la passphrase, confermare la passphrase e cliccare su **OK**.
2. Per cifrare altri file con la chiave appena impostata, selezionare **Cifra** dal menu di scelta rapida o dal menu **File**.
   L'ultima chiave utilizzata e impostata da SafeGuard Portable verrà utilizzata per tutti i processi di cifratura successivi eseguiti con SafeGuard Portable, a meno che non venga impostata una chiave nuova.

4.15.3 Decifratura di file con SafeGuard Portable

1. In SafeGuard Portable, cliccare con il tasto destro del mouse sul file e selezionare **Decifra**.

   Viene visualizzata la finestra per l'immissione della passphrase dei supporti o della passphrase di una chiave locale.
2. Immettere la passphrase appropriata (la passphrase deve essere fornita dal mittente) e cliccare su **OK**.

   Il file è stato decifrato.

La passphrase dei supporti rimovibili consente di accedere a tutti i file cifrati, indipendentemente dalla chiave locale utilizzata per cifrarli. Se si dispone solo della passphrase di una chiave locale, sarà possibile accedere solamente ai file che sono stati cifrati con questa chiave.

Quando si decifra un file che è stato cifrato utilizzando una chiave generata in SafeGuard Portable, tale file viene decifrato automaticamente.

Dopo aver decifrato i file e aver immesso la passphrase della chiave, non sarà necessario immettere alcuna passphrase la prossima volta che verranno cifrati o decifrati utilizzando la stessa chiave.

SafeGuard Portable memorizza la passphrase durante l'intera durata dell'esecuzione dell'applicazione. Per la cifratura viene adoperata l'ultima chiave utilizzata da SafeGuard Portable.

I file decifrati vengono nuovamente cifrati alla chiusura di SafeGuard Portable.

5 Supporto

Versione completa

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.

6 Note legali