SOPHOS

Cybersecurity made simple.

Sophos Central Device Encryption

Guida per amministratori

Sommario

1 Info su Sophos Central Device Encryption

Sophos Central Device Encryption consente di gestire la Crittografia unità BitLocker sugli endpoint Windows e la crittografia FileVault su endpoint Mac tramite Sophos Central.

La cifratura degli hard disk garantisce la sicurezza dei dati, anche in caso di furto o smarrimento di un dispositivo.

Questa guida descrive come impostare e utilizzare la cifratura dei dispositivi. Inoltre, indica come recuperare la chiave di ripristino con il portale self-service. Per informazioni dettagliate sulle impostazioni dei criteri, sugli avvisi e sul ripristino con Sophos Central, vedere la Guida in linea di Sophos Central.

Informazioni correlate

Guida in linea di Sophos Central

2 Gestione della Crittografia unità BitLocker

Questa sezione descrive i prerequisiti per l'uso della Crittografia unità BitLocker negli endpoint Windows presenti all'interno della rete, oltre alle varie modalità di autenticazione disponibili e a come interagiscono con le impostazioni interne dei criteri di gruppo.

2.1 Migrazione a Sophos Central Device Encryption

Se si utilizza già SafeGuard Enterprise con la Crittografia unità BitLocker o Sophos Full Disk Encryption, questa sezione indica come effettuare la migrazione a Sophos Central Device Encryption.

Include:

- SafeGuard Enterprise e BitLocker
- SafeGuard Enterprise e Sophos Full Disk Encryption
- Per informazioni sulla migrazione degli endpoint Mac, vedere Migrazione a Sophos Central Device Encryption (Mac).

Attività correlate

Migrazione a Sophos Central Device Encryption (Mac) (pagina 14)
Se si desidera utilizzare Sophos Central per gestire endpoint Mac che sono già stati cifrati con FileVault, occorrerà applicare un criterio Sophos Central Device Encryption agli endpoint interessati.

2.1.1 Migrazione da SafeGuard Enterprise BitLocker

Per eseguire la migrazione, procedere come segue.

Nota
Se si utilizza BitLocker con SafeGuard Enterprise versione 6.x o 7.x, si consiglia di effettuare prima l'upgrade all'ultima versione di SafeGuard Enterprise.

Se si utilizza SafeGuard Enterprise versione 6.x o 7.x, occorre decifrare il disco di sistema seguendo la procedura descritta nella Guida in linea per amministratori di SafeGuard Enterprise, prima di poter migrare a Sophos Central Device Encryption.

Per migrare da SafeGuard Enterprise BitLocker Client (versione 8.0 o successiva) a Sophos Central Device Encryption:

1. Selezionare **Pannello di controllo > Disinstalla un programma** e cliccare con il tasto destro del mouse su **Sophos SafeGuard Client**.
2. Selezionare **Cambia** dal menù del tasto destro del mouse.
   Si aprirà la procedura guidata per l'impostazione di Sophos SafeGuard Client.
3. Disinstallare il componente BitLocker.

Nota
La rimozione del componente BitLocker non decifrerà né volumi né file.

4. Installare il software Sophos Central Device Encryption.
5. Verificare che sia stato assegnato e attivato nell'endpoint un criterio Sophos Central Device Encryption.

Sarà ora possibile gestire BitLocker con Sophos Central. Non sarà necessario effettuare nuovamente la cifratura. Una volta applicato un criterio Sophos Central Device Encryption all'endpoint, la chiave di ripristino verrà rinnovata e inviata a Sophos Central. La funzionalità di cifratura dei file non subirà alcuna modifica.

Informazioni correlate
SafeGuard Enterprise Guida in linea per amministratori (in inglese)

2.1.2 Migrazione da SafeGuard Enterprise Full Disk Encryption

Per eseguire la migrazione, procedere come segue.

Per migrare da SafeGuard Enterprise Full Disk Encryption:

1. Disinstallare il software Sophos SafeGuard Client.
   I volumi cifrati verranno decifrati automaticamente. I file cifrati rimarranno cifrati.
2. Installare il software Sophos Central Device Encryption.
3. Verificare che sia stato assegnato e abilitato nell'endpoint un criterio Sophos Central Device Encryption.
4. Re-installare il modulo di SafeGuard Enterprise File Encryption richiesto (cifratura sincronizzata o cifratura dei file basata sul percorso).

Sarà ora possibile gestire BitLocker con Sophos Central. Una volta applicato un criterio Sophos Central Device Encryption all'endpoint, la cifratura si avvierà in background e la chiave di ripristino verrà rinnovata e inviata a Sophos Central.

2.2 Preparazione di Device Encryption

Per impostazione predefinita, la maggior parte delle unità di sistema viene preparata per BitLocker. Se così non dovesse essere, Sophos Central Device Encryption eseguirà automaticamente lo strumento a riga di comando Microsoft `BdeHdCfg.exe` per preparare l'unità.

Ciò significa che nell'unità di sistema viene creata una partizione indipendente per BitLocker.

Durante l'impostazione di Sophos Central Device Encryption, un messaggio comunicherà all'utente che è richiesto un riavvio per preparare l'unità di sistema. L'utente può riavviare il computer immediatamente, oppure posticipare l'operazione. Device Encryption può cominciare solamente quando il computer viene riavviato e la preparazione dell'unità di sistema è stata completata.

La versione di .NET Framework richiesta da Device Encryption viene installata automaticamente negli endpoint.

2.3 Device Encryption passo per passo

Per cifrare i dispositivi, procedere come segue.

Prima che gli utenti possano cominciare:

- Il software dell'agente di Sophos Central deve essere installato sugli endpoint.
- Occorre configurare un criterio di Device Encryption in Sophos Central.
- Gli utenti devono accedere ai propri endpoint in maniera interattiva, effettuandone la connessione e sincronizzazione con Sophos Central. Si prega di notare che l'accesso remoto non è supportato.
- Il sistema operativo deve supportare la funzionalità Crittografia unità BitLocker. Per maggiori informazioni, consultare le sezioni Preparazione di Device Encryption e Compatibilità di sistema per Device Encryption.

Queste istruzioni indicano cosa vedono gli utenti, e come devono procedere:

1. Se l'hardware di sicurezza TPM non è ancora stato abilitato, viene attivata un'azione BIOS per abilitarlo. Questo processo richiede un riavvio. L'utente può effettuare il riavvio immediatamente, oppure posticiparlo.
   Durante il riavvio, all'utente verrà richiesto di abilitare TPM. Nel caso non fosse possibile abilitare TPM, oppure se l'utente non dovesse rispondere, verrà visualizzato un messaggio.
2. Se il TPM è attivo e abilitato ma non è associato a un proprietario, il software dell'agente di Sophos Central genererà e imposterà automaticamente le informazioni del proprietario del TPM. Se questa operazione non dovesse riuscire, verrà inviata una notifica a Sophos Central.
3. Se dovessero mancare le chiavi di verifica dell'autenticità del TPM, il software dell'agente di Sophos Central le creerà automaticamente. Se questa operazione non dovesse riuscire, verrà inviata una notifica a Sophos Central.
4. Se il criterio di Device Encryption non specifica l'opzione **Richiedi autenticazione all'avvio**, la cifratura dell'hard disk si avvierà automaticamente. In tale eventualità, gli utenti non dovranno intraprendere alcuna azione. È possibile passare al punto 8.
5. Se il criterio di Device Encryption invece specifica l'opzione **Richiedi autenticazione all'avvio**, si aprirà la finestra di dialogo **Sophos Device Encryption**.
   - Se il criterio di Device Encryption richiede un PIN o una password per l'autenticazione, seguire le istruzioni visualizzate sullo schermo per impostare un PIN o una password. Se viene utilizzato TPM+PIN, la chiave di cifratura per il disco di sistema verrà memorizzata nel TPM.

     Nota
     Gli utenti dovranno prestare estrema attenzione quando impostano 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.

   - Se il criterio di Device Encryption richiede una chiave USB per l'autenticazione, gli utenti dovranno connettere un'unità flash USB al computer. L'unità flash USB deve essere formattata con NTFS, FAT, o FAT32.
6. Quando l'utente clicca su **Riavvia e cifra**, il computer si riavvierà e verificherà il corretto funzionamento di Device Encryption.
   L'utente può selezionare **Rimanda a un altro momento** per chiudere la finestra di dialogo. Tuttavia, comparirà nuovamente all'accesso successivo dell'utente, oppure quando verrà modificato il criterio Device Encryption.

7. Se l'utente non fosse in grado di inserire il giusto PIN o la giusta password, potrà cliccare sul tasto `Esc`. Il sistema si avvierà normalmente, in quanto la cifratura non è ancora stata applicata. All'utente verrà richiesto di inserire nuovamente PIN/password dopo l'accesso.
8. Gli amministratori possono vedere quali sono gli utenti che non hanno ancora abilitato la cifratura. Significa che questi utenti non hanno ancora riavviato il computer e non hanno ancora seguito le istruzioni visualizzate sullo schermo. Cercare nei **Report** in Sophos Central.
9. Se il test di preavvio fornisce il risultato desiderato, il software dell'agente di Sophos Central avvierà la cifratura dei dischi rigidi. La cifratura avviene in background, per cui consente agli utenti di utilizzare il proprio computer come di consueto.
   Se il test dell'hardware dovesse dare esito negativo, il sistema si riavvierà e la cifratura non verrà implementata. L'amministratore riceverà un evento di notifica in Sophos Central.
10. Una volta completata la cifratura del volume di sistema da parte dell'agente di Sophos Central, verrà avviata la cifratura dei volumi di dati (se specificato nel criterio). La protezione di questi volumi verrà archiviata nel volume di sistema, per cui i volumi di dati saranno disponibili automaticamente subito dopo l'avvio. Ciò significa che, quando un utente effettua l'accesso al proprio computer, sarà possibile accedere ai volumi di dati senza altra interazione da parte dell'utente. I volumi di dati rimovibili, come ad es. le unità flash USB, non vengono cifrati.

I due file di log `CDE.log` e `CDE_trace.xml` sono reperibili nell'endpoint, al percorso `%ProgramData%\Sophos\Sophos Data Protection\Logs`.

Concetti correlati

Preparazione di Device Encryption (pagina 3)
Per impostazione predefinita, la maggior parte delle unità di sistema viene preparata per BitLocker. Se così non dovesse essere, Sophos Central Device Encryption eseguirà automaticamente lo strumento a riga di comando Microsoft `BdeHdCfg.exe` per preparare l'unità.

Compatibilità di sistema per Device Encryption (pagina 5)
La tabella che segue fornisce una panoramica dei tipi di protezione supportati sulle varie piattaforme. Il tipo di protezione applicato dipende dalla versione di Windows in uso, e dalla disponibilità o meno dell'hardware di sicurezza TPM.

TPM+PIN (pagina 7)
La modalità TPM+PIN utilizza come metodo di autenticazione l'hardware di sicurezza TPM del computer e un PIN.

2.4 Compatibilità di sistema per Device Encryption

La tabella che segue fornisce una panoramica dei tipi di protezione supportati sulle varie piattaforme. Il tipo di protezione applicato dipende dalla versione di Windows in uso, e dalla disponibilità o meno dell'hardware di sicurezza TPM.

Il numero tra parentesi indica la priorità del tipo specifico di protezione.

(*) Quando è attivata l'opzione **Richiedi autenticazione all'avvio**, non è possibile installare la protezione TPM-only, per cui TPM+PIN assumerà la priorità più elevata.

	Win 7 no TPM	Win 7 con TPM	Win 8.1 no TPM	Win 8.1 con TPM	Win 10 no TPM	Win 10 con TPM
TPM-only	-	ok (1*)	-	ok (1*)	-	ok (1*)
TPM+PIN	-	ok (2)	-	ok (2)	-	ok (2)

	Win 7 no TPM	Win 7 con TPM	Win 8.1 no TPM	Win 8.1 con TPM	Win 10 no TPM	Win 10 con TPM
Passphrase	-	-	ok (1)	ok (3)	ok (1)	ok (3)
USB key	ok (1)	ok (3)	-	-	-	-

Quando si utilizza Central Device Encryption, potrebbe essere necessario configurare il TPM sul computer endpoint.

Se si utilizza TPM 2.0 o versione successiva, è necessario formattare il disco rigido, in quanto il GPT e il BIOS devono essere in modalità UEFI.

Se si utilizza TPM 1.2, il TPM deve essere attivato nel BIOS/UEFI e deve essere pronto per l'uso. È possibile verificare queste condizioni utilizzando `TPM.MSC`.

Si consiglia di aggiornare i computer endpoint alla versione più recente del BIOS/UEFI prima di installare Central Device Encryption.

Quando è abilitata la modalità Windows FIPS, la cifratura BitLocker è supportata solamente nei sistemi con Windows 8.1 o Windows 10. Per informazioni dettagliate su BitLocker in modalità FIPS su Windows 7, vedere Impossibile salvare una password di ripristino compatibile con FIPS di dominio Active Directory per BitLocker in Windows 7 o Windows Server 2008 R2.

con Sophos Central Device Encryption è possibile utilizzare dischi rigidi cifrati. Per ulteriori informazioni, vedere Disco rigido cifrato.

Central Device Encryption supporta BitLocker con pre-provisioning.

Informazioni correlate

Impossibile salvare una password di ripristino compatibile con FIPS di dominio Active Directory per BitLocker in Windows 7 o Windows Server 2008 R2

Disco rigido cifrato

2.5 Modalità di autenticazione della cifratura dei dispositivi

È possibile utilizzare lo switch **Richiedi autenticazione all'avvio** nelle impostazioni della cifratura dei dispositivi per determinare se gli utenti debbano autenticarsi quando accedono ai propri computer.

La modalità di autenticazione installata sui computer dipende dal sistema, dalle impostazioni del criterio di gruppo per BitLocker e dal criterio di Device Encryption configurato. A seconda della compatibilità di sistema per Device Encryption, sugli endpoint verrà installata una delle seguenti modalità di autenticazione:

- TPM+PIN
- Passphrase
- TPM-only
- USB key

Sugli endpoint che sono già cifrati con BitLocker, un messaggio indicherà agli utenti i passaggi da svolgere.

Quando viene attivata **Richiedi autenticazione all'avvio**, verrà richiesto agli utenti di impostare un PIN / passphrase / chiave USB, e cliccare su **Applica**. Successivamente, dovranno utilizzare questo

PIN / passphrase / chiave USB a ogni avvio del computer. Disattivando **Richiedi autenticazione all'avvio**, verrà automaticamente applicata la modalità TPM-only, senza che sia richiesto alcun altro tipo di autenticazione. Agli utenti verrà comunicato che il computer sbloccherà automaticamente il dispositivo all'avvio.

Sophos Device Encryption può configurare automaticamente l'oggetto criteri di gruppo (GPO) in modo da autorizzare tutte le modalità di autenticazione, a patto che l'impostazione corrispondente risulti come **not configured** (non configurata). Quando questa impostazione viene configurata manualmente, il software non sovrascriverà quanto specificato. Per maggiori informazioni, vedere Impostazioni del criterio di gruppo per BitLocker.

Gli utenti possono scegliere di posticipare l'installazione delle modalità di autenticazione. In questo caso non verrà effettuata alcuna cifratura. Ogni volta che un utente effettua nuovamente l'accesso a Windows, oppure quando viene distribuito un nuovo criterio di cifratura, il sistema richiederà all'utente di riavviare il computer. Dopo il riavvio, verrà installata la modalità di autenticazione, e comincerà la cifratura dei dispositivi. Dopo questa operazione, gli utenti non saranno in grado di decrittografare i propri dispositivi.

Concetti correlati

Compatibilità di sistema per Device Encryption (pagina 5)
La tabella che segue fornisce una panoramica dei tipi di protezione supportati sulle varie piattaforme. Il tipo di protezione applicato dipende dalla versione di Windows in uso, e dalla disponibilità o meno dell'hardware di sicurezza TPM.

Impostazioni del criterio di gruppo per BitLocker (pagina 9)
Sophos Central definisce automaticamente alcune impostazioni dei criteri di gruppo, per cui gli amministratori non devono necessariamente preparare i computer per la cifratura dei dispositivi.

2.5.1 TPM+PIN

La modalità TPM+PIN utilizza come metodo di autenticazione l'hardware di sicurezza TPM del computer e un PIN.

Gli utenti devono inserire questo PIN nell'ambiente di preavvio di Windows a ogni avvio del computer.

TPM+PIN richiede la preparazione di un TPM, e le impostazioni del GPO (oggetto criteri di gruppo) del sistema devono autorizzare la modalità TPM+PIN.

Se vengono soddisfatte tutte le condizioni, verrà visualizzata la finestra di dialogo per l'impostazione di TPM+PIN, e all'utente verrà richiesto di specificare un PIN. L'utente può cliccare su **Riavvia e cifra** per riavviare immediatamente il computer e cominciare la cifratura.

Se è abilitata l'impostazione **Consenti PIN avanzati per l'avvio** del GPO, il PIN può includere cifre, lettere e caratteri speciali. Altrimenti sarà consentito solamente l'utilizzo di caratteri numerici.

Il PIN di BitLocker è di una lunghezza compresa tra 4 e 20 caratteri. È possibile definire una lunghezza minima maggiore, impostando un criterio di gruppo. Il software dell'agente di Sophos Central imposta il criterio di gruppo in modo da consentire l'utilizzo di PIN avanzati. La finestra di dialogo indica all'utente quali caratteri possano essere inseriti, e quali siano le lunghezze minime/massime consentite.

Nota
Tutti gli utenti di un computer Windows specifico dovranno avere lo stesso PIN per sbloccare il disco di sistema, dopodiché effettueranno l'accesso al sistema operativo con le proprie credenziali individuali. Il single sign-on non è supportato per i computer Windows.

2.5.2 Passphrase

Per l'autenticazione sugli endpoint che non sono dotati di hardware di sicurezza TPM, è possibile utilizzare una passphrase.

Gli utenti dovranno inserire questa passphrase nell'ambiente di preavvio di Windows a ogni avvio del computer.

La protezione con passphrase richiede Windows versione 8.0 o successive, e le impostazioni dell'oggetto criteri di gruppo (GPO) del sistema devono consentire la modalità passphrase.

Se vengono soddisfatte tutte le condizioni, verrà visualizzata la finestra di dialogo di impostazione della modalità passphrase, e all'utente verrà richiesto di impostare una passphrase della lunghezza di 8-100 caratteri. L'utente può cliccare su **Riavvia e cifra** per riavviare immediatamente il computer e cominciare la cifratura.

2.5.3 Solo TPM

La modalità TPM-only utilizza l'hardware di sicurezza TPM del computer senza alcuna autenticazione tramite PIN.

Ciò significa che l'utente può avviare il computer senza alcuna richiesta di inserire un PIN nell'ambiente di preavvio di Windows.

TPM-only richiede la preparazione di un TPM, e l'impostazione del criterio **Richiedi autenticazione all'avvio** di Cifratura dei dispositivi deve essere disattivata. Inoltre, le impostazioni dell'oggetto criteri di gruppo (GPO) del sistema devono consentire la protezione TPM-only.

Se vengono soddisfatte tutte le condizioni, verrà visualizzata la finestra di dialogo della protezione TPM-only. L'utente può cliccare su **Riavvia e cifra** per riavviare immediatamente il computer e cominciare la cifratura.

2.5.4 USB key

La modalità USB key effettua l'autenticazione utilizzando una chiave archiviata su un'unità flash USB.

Per ciascun riavvio, occorrerà che l'unità flash USB sia connessa al computer.

La protezione con chiave USB viene adoperata solamente su endpoint Windows 7 quando non è disponibile alcun tipo di TPM, oppure se il TPM è stato disattivato tramite GPO (oggetto criteri di gruppo).

L'unità flash USB deve essere formattata con NTFS, FAT, o FAT32. Il formato exFAT non è supportato. Inoltre, l'unità flash USB deve essere scrivibile.

Se vengono soddisfatte tutte le condizioni, comparirà la finestra di dialogo dell'installazione della protezione tramite chiave USB, e l'utente dovrà selezionare un'unità flash USB su cui archiviare la chiave.

L'utente può cliccare su **Riavvia e cifra** per riavviare immediatamente il computer e cominciare la cifratura.

2.6 Impostazioni del criterio di gruppo per BitLocker

Sophos Central definisce automaticamente alcune impostazioni dei criteri di gruppo, per cui gli amministratori non devono necessariamente preparare i computer per la cifratura dei dispositivi.

Se gli amministratori dovessero già aver definito le impostazioni, i valori configurati non verranno sovrascritti.

In **Editor Criteri di gruppo locali**, sotto **Configurazione computer > Modelli amministrativi > Componenti di Windows > Crittografia unità BitLocker > Unità del sistema operativo**, vengono visualizzati i seguenti criteri:

Criterio	Impostazione	Valore impostato da Sophos Central	Commento
Consenti sblocco rete all'avvio		Abilitata	Uno sblocco di rete preconfigurato di BitLocker può essere mantenuto attivo dopo l'abilitazione di Central Device Encryption.
Richiedi autenticazione aggiuntiva all'avvio	Consenti BitLocker senza un TPM compatibile	Spuntata	Questa opzione viene impostata per Windows 8 se non è disponibile alcun TPM, al fine di consentire l'uso di una password all'avvio, per sbloccare il disco di sistema.
Richiedi autenticazione aggiuntiva all'avvio	Configurazione PIN di avvio del TPM	Consenti PIN di avvio con il TPM	Se viene definita l'impostazione del criterio **Richiedi autenticazione all'avvio** per Device Encryption e il sistema dispone di un TPM, questa impostazione dei criteri di gruppo consentirà la protezione dell'unità di sistema tramite TPM, richiedendo all'utente anche l'inserimento di un PIN.
Consenti PIN avanzati per l'avvio	N.d.	Abilitata	Questa opzione viene impostata per permettere l'utilizzo di PIN alfanumerici, al fine di proteggere l'unità di sistema tramite TPM. Qualora non potesse essere impostata, verrà consentito solamente l'uso di caratteri numerici.
Configura il messaggio e l'URL di recupero prima dell'avvio	Selezionare un'opzione per il messaggio di recupero prima dell'avvio	Usa il messaggio e l'URL di recupero predefiniti	Questa opzione viene impostata in modo da utilizzare il messaggio predefinito e l'URL di Sophos.

Criterio	Impostazione	Valore impostato da Sophos Central	Commento
Configura il messaggio e l'URL di recupero prima dell'avvio	Opzione messaggio di recupero personalizzato	Non si dispone di una password di ripristino? Contattare il supporto tecnico o visitare il proprio Portale self-service: `https://sophos.com/ssp`	
Configura il messaggio e l'URL di recupero prima dell'avvio	Opzione URL di recupero personalizzato		
Configura utilizzo della crittografia hardware per unità dati fisse	n.d.	Disattivato	Questa opzione è impostata in modo da implementare la cifratura basata su software. Tuttavia, se l'impostazione di un criterio di gruppo di BitLocker già esistente richiede la cifratura basata su hardware, l'impostazione di quel criterio non verrà sovrascritta.
Configura utilizzo della crittografia hardware per unità del sistema operativo	n.d.	Disattivato	Questa opzione è impostata in modo da implementare la cifratura basata su software. Tuttavia, se l'impostazione di un criterio di gruppo di BitLocker già esistente richiede la cifratura basata su hardware, l'impostazione di quel criterio non verrà sovrascritta.

- Encryption algorithm to be used (Algoritmo di cifratura da utilizzare): per impostazione predefinita, Sophos Central Device Encryption utilizza AES-256. È presente un'impostazione del criterio di gruppo che può essere adoperata per selezionare AES-128.
- PIN/password requirements (Requisiti PIN/password): vi sono impostazioni del criterio di gruppo che possono essere utilizzate per stabilire una lunghezza minima per PIN/password, e per richiedere l'uso di password complesse.
- Encrypt all data or used space only (Cifratura di tutti i dati o solamente dello spazio utilizzato): Se il criterio di gruppo dei volumi di avvio e/o dei volumi di dati è impostato in modo da richiedere la cifratura completa dei dati, assumerà la priorità rispetto a qualsiasi criterio Sophos Central che permetta solamente la cifratura dello spazio utilizzato.

Alcune impostazioni del criterio di gruppo potrebbero trovarsi in conflitto con Sophos Central, per cui non sarà possibile abilitare la cifratura. In tale eventualità, verrà inviato un evento a Sophos Central.

- Smart card required (Smart Card obbligatoria): se un criterio di gruppo dovesse richiedere l'utilizzo di una smart card per BitLocker, questa opzione non sarà supportata da Sophos Central, per cui genererà un evento di errore.
- Encrypt all data or used space only (Cifratura di tutti i dati o solamente dello spazio utilizzato): se il criterio di gruppo per i volumi di avvio e/o i volumi di dati è impostato in modo da cifrare solamente lo spazio utilizzato, ma il criterio di Sophos Central richiede la cifratura completa, questo conflitto genererà un evento di errore.

Se si desidera cifrare dispositivi tablet (come ad es. MS Surface Pro) e utilizzare l'autenticazione all'avvio, occorre abilitare la seguente impostazione dei criteri di gruppo:

Abilita l'uso dell'autenticazione BitLocker che richiede l'input da tastiera prima dell'avvio negli slate

Per ulteriori informazioni, consultare l'articolo 125772 della knowledge base.

Per ulteriori informazioni generali sulle impostazioni dei criteri di gruppo di BitLocker e TPM, vedere Impostazioni del criterio di gruppo per BitLocker e Impostazioni del criterio di gruppo dei servizi Trusted Platform Module.

Concetti correlati

Metodo di cifratura e reportistica (pagina 11)
I volumi possono essere crittografati con cifratura basata su software o cifratura basata su hardware.

Informazioni correlate

Impostazioni del criterio di gruppo per BitLocker

Impostazioni del criterio di gruppo per TPM

Articolo 125772 della knowledge base

2.7 Limitazioni

Dischi dinamici

BitLocker non supporta i dischi dinamici. Gli endpoint inviano un evento a Sophos Central per comunicare che non è stato possibile effettuare la cifratura. Ciò è dovuto al fatto che un volume di sistema su un disco dinamico non può essere cifrato. I volumi di dati nei dischi dinamici vengono semplicemente ignorati.

Desktop remoto

Quando si utilizza la funzionalità Desktop remoto per un endpoint Windows su cui è installato il software dell'agente di Sophos Central, qualora dovesse essere stato impostato un criterio di cifratura, il sistema non visualizzerà alcuna finestra di dialogo e la cifratura del dispositivo NON verrà implementata. L'abilitazione della cifratura attiverà in una sequenza di riavvio per verificare la compatibilità dell'hardware. L'utente dovrà essere in grado di inserire PIN / passphrase nell'ambiente di preavvio, e questa operazione non può essere effettuata con Desktop remoto.

2.8 Metodo di cifratura e reportistica

I volumi possono essere crittografati con cifratura basata su software o cifratura basata su hardware.

Device Encryption utilizza sempre la cifratura basata su software per i nuovi volumi, anche se l'unità supporta la cifratura basata su hardware.

Se un'unità è già crittografata con cifratura basata su hardware, non verrà modificata.

Se l'impostazione di un criterio di gruppo di BitLocker richiede la cifratura basata su hardware, non verrà modificata.

Nella pagina **Computer** è possibile filtrare i computer ad es. in base al relativo stato di cifratura, al metodo di cifratura o ai computer che non sono cifrati.

La pagina dei dettagli di un computer mostra il metodo di cifratura e l'algoritmo utilizzati per un volume.

Per i computer Windows, può anche essere visualizzato **Cifrato da**. Le informazioni indicate dipendono dal dispositivo.

- Per i computer già cifrati con Sophos Central Device Encryption, vengono visualizzate la data e l'ora in cui il computer ha effettuato l'upgrade a Central Device Encryption versione 2.1.
- Per i computer cifrati con un altro prodotto, vengono visualizzate la data e l'ora di installazione di Sophos Central Device Encryption.
- Per i nuovi computer cifrati con Sophos Central Encryption 2.1 (o versione successiva), vengono visualizzate la data e l'ora della cifratura.

Il report **Stato di cifratura** mostra lo stato di cifratura dei computer.

Indica quali computer e quali tipi di volume sono cifrati, nonché quali computer sono conformi ai criteri di cifratura. Inoltre, fornisce informazioni relative a come si autenticano e come vengono cifrati i propri computer.

Concetti correlati

Impostazioni del criterio di gruppo per BitLocker (pagina 9)
Sophos Central definisce automaticamente alcune impostazioni dei criteri di gruppo, per cui gli amministratori non devono necessariamente preparare i computer per la cifratura dei dispositivi.

Computer

Riepilogo del computer

2.9 Informazioni sulla decifratura

Solitamente non occorre effettuare la decifratura. Un endpoint cifrato può essere escluso dalla cifratura rimuovendone tutti gli utenti dal criterio e successivamente disattivando la cifratura.

In Esplora risorse (sull'endpoint), cliccare con il tasto destro del mouse sul disco di sistema e selezionare **Gestione BitLocker**. Nella finestra di dialogo **Crittografia unità BitLocker**, cliccare su **Disattiva BitLocker**. Solamente un amministratore Windows sarà in grado di effettuare questa operazione.

Se è stato applicato un criterio di cifratura e un utente con privilegi di amministrazione dovesse cercare di decifrare manualmente il proprio disco rigido, Sophos Central assumerà la priorità rispetto al comando dell'utente e il disco rimarrà cifrato.

2.10 Ripristino di endpoint Windows

Se gli utenti dovessero dimenticare il proprio PIN o password di BitLocker, hanno a disposizione due modi per recuperare nuovamente l'accesso ai propri computer.

- Gli utenti possono accedere al portale self-service di Sophos, vedere Recupero della chiave di ripristino tramite portale self-service. Gli utenti Windows 10 riceveranno istruzioni nella schermata **Ripristino BitLocker**.

- L’amministratore può aiutare l’utente ad accedere al proprio computer. Queste istruzioni indicano cosa vedono gli utenti e come devono procedere. Dovranno:

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**.
3. Contattare l’amministratore e fornire l’ID chiave di ripristino.
   L’amministratore può fornire la chiave di ripristino. Per assistenza durante il recupero della chiave di uno degli utenti, consultare la Guida in linea di Sophos Central.
4. L’utente deve inserire la chiave di ripristino e seguire le istruzioni visualizzate sullo schermo per creare un nuovo PIN o password.

   I computer che eseguono Windows 7 non visualizzano istruzioni. La reimpostazione del PIN o della password deve essere effettuata manualmente.

Gli utenti potranno nuovamente accedere al proprio computer. Solitamente i volumi di dati vengono sbloccati manualmente non appena l'utente è in grado di accedere al volume di avvio. Se ciò non dovesse avvenire, è possibile ottenere una chiave di ripristino per il volume di dati in Sophos Central, procedendo nella stessa maniera applicabile ai volumi di avvio.

Attività correlate

Recupero della chiave di ripristino tramite portale self-service (pagina 22)
Se gli utenti non dovessero essere in grado di accedere ai propri computer (ad es. nel caso in cui abbiano dimenticato il PIN di BitLocker, la password di macOS, ecc.), potranno adoperare il Sophos Self Service Portal per recuperare una chiave di ripristino.

Informazioni correlate

Portale self-service

Guida in linea di Sophos Central

3 Gestione della crittografia FileVault

Sophos Central Device Encryption per Mac gestisce la funzionalità di cifratura completa del disco FileVault sui Mac.

Gli utenti avranno solamente bisogno della propria password di accesso di macOS per cifrare e accedere ai propri dati.

3.1 Migrazione a Sophos Central Device Encryption (Mac)

Se si desidera utilizzare Sophos Central per gestire endpoint Mac che sono già stati cifrati con FileVault, occorrerà applicare un criterio Sophos Central Device Encryption agli endpoint interessati.

Nota
Se si utilizza FileVault con SafeGuard Enterprise, occorrerà prima disinstallare il software **Sophos SafeGuard Device Encryption**.

Prima che gli utenti possano cominciare:

- È necessario installare il software dell'agente di Sophos Central sugli endpoint.
- Occorre configurare e attivare un criterio di Device Encryption in Sophos Central.
- Gli utenti devono aver effettuato l'accesso ai propri endpoint. Devono essere connessi e sincronizzati con Sophos Central. Si prega di notare che l'accesso remoto non è supportato.

Queste istruzioni indicano cosa vedono gli utenti, e come devono procedere:

1. Quando un utente effettua l'accesso, o quando si applica un criterio Sophos Central Device Encryption dopo che un utente ha effettuato l'accesso, verrà visualizzato all'utente un messaggio che indica che è stata impostata la cifratura dei dispositivi per la protezione del proprio computer.
2. Per attivare Sophos Central Device Encryption, gli utenti dovranno inserire la propria password di accesso e cliccare su **Crea chiave**.
   Verrà quindi creata e memorizzata centralmente una nuova chiave di ripristino a scopo di ripristino. Nel caso in cui vi siano altri dischi interni non cifrati, anche questi ultimi verranno cifrati. Non occorrerà una password diversa per questi dischi.
3. Se sono presenti dischi interni che sono già stati cifrati con una password del disco, gli utenti dovranno inserire la propria password del disco e cliccare su **Procedi**.
   La password del disco è ora gestita da Sophos Central. Il disco verrà automaticamente sbloccato in fase di avvio.

L'endpoint sarà ora gestito da Sophos Central Device Encryption.

3.2 La cifratura dei dispositivi passo per passo (Mac)

Per cifrare i Mac, procedere come segue.

Prima che gli utenti possano cominciare:

- È necessario installare il software dell'agente di Sophos Central sugli endpoint.
- Occorre configurare e attivare un criterio di Device Encryption in Sophos Central.
- Gli utenti devono aver effettuato l'accesso ai propri endpoint. Devono essere connessi e sincronizzati con Sophos Central. Si prega di notare che l'accesso remoto non è supportato.

Queste istruzioni indicano cosa vedono gli utenti e come devono procedere.

1. Immettere la propria password di accesso, dopo aver avviato il proprio Mac.

   Questa operazione attiva Sophos Device Encryption.
2. Cliccare su **Cifra** per avviare la cifratura del disco di sistema, oppure su **Posponi** per avviare il processo in un secondo momento.

   Quando un utente inserisce la propria password di accesso e clicca su **Cifra**, la chiave di ripristino verrà memorizzata localmente nel portachiavi e in Sophos Central.

   Tutti gli utenti già esistenti di un endpoint vengono automaticamente aggiunti a FileVault.

   Negli endpoint che eseguono macOS 10.12 o versioni precedenti, ciascun utente deve effettuare l'accesso separatamente per essere aggiunto a FileVault.

Quando viene cifrato il disco di sistema, i volumi di dati interni saranno automaticamente cifrati. I dischi cifrati vengono automaticamente sbloccati al riavvio del computer.

Le notifiche forniscono agli utenti informazioni sullo stato di cifratura dei singoli dispositivi.

3.2.1 Aggiunta di nuovi utenti FileVault

Se gli utenti non vengono aggiunti automaticamente a FileVault, queste istruzioni descrivono cosa vedono i nuovi utenti e come devono procedere.

Dovranno:

1. Immettere la propria password di accesso e cliccare su **Procedi**.
   Normalmente gli utenti possono utilizzare la propria password di accesso di macOS per accedere al Mac e adoperare FileVault.
2. Se non è ancora stata memorizzata alcuna chiave di ripristino in Sophos Central, i nuovi utenti dovranno selezionare un utente FileVault già esistente che sia in grado di autorizzare questa operazione.
3. L'utente FileVault già esistente dovrà quindi inserire la propria password di accesso e cliccare su **Procedi**.

I nuovi utenti potranno ora utilizzare la propria password di accesso di macOS per accedere al Mac e adoperare FileVault.

3.3 Ripristino di endpoint Mac

Per ripristinare i Mac, procedere come segue.

Se un utente dovesse dimenticare la propria password di accesso, esistono diversi modi per poter accedere nuovamente al proprio computer.

- Se l'utente è stata l'ultima persona ad accedere al computer, può adoperare il portale self-service di Sophos, vedere Recupero della chiave di ripristino tramite portale self-service.
- Gli utenti possono avviare i computer con un disco di avvio esterno per Mac, e successivamente adoperare i comandi del Terminal per sbloccare il disco.

- Gli utenti possono avviare i computer in modalità disco di destinazione e successivamente adoperare i comandi del Terminal per sbloccare il disco.
- Gli utenti possono avviare i computer in modalità macOS Recovery e successivamente adoperare i comandi del Terminal per sbloccare il disco.

  Per informazioni sull'utilizzo dei comandi Terminal, vedere Sblocco dei volumi HFS+ mediante i comandi del Terminal e Sblocco dei volumi APFS mediante i comandi del Terminal.

L'amministratore può aiutare gli utenti a recuperare l'accesso. Queste istruzioni indicano cosa vedono gli utenti e come devono procedere. Dovranno:

1. Accendere il proprio endpoint e attendere che venga visualizzato l'**ID chiave di ripristino**.
   l'ID chiave di ripristino verrà visualizzato solamente per pochi minuti. Per visualizzarlo nuovamente, gli utenti dovranno riavviare il computer.
2. Contattare l'amministratore e fornire l'ID chiave di ripristino.
   L'amministratore può fornire la chiave di ripristino. Per assistenza durante il recupero della chiave di uno degli utenti, consultare la Guida in linea di Sophos Central.
3. Cliccare sull'icona a forma di punto interrogativo nel campo **Password**.
   Verrà visualizzato un messaggio.
4. Cliccare sull'icona a forma di freccia accanto al messaggio per passare al campo delle chiave di ripristino.
5. Inserire la chiave di ripristino.

   Per gli utenti importati da Active Directory, occorre completare anche la seguente procedura aggiuntiva:

   - Reimpostare la password attuale in Active Directory. Generare quindi una password preliminare e fornirla all'utente.
   - Indicare all'utente di premere su **Annulla** nella finestra di dialogo **Reimposta password** e di immettere la password preliminare.
6. Seguire le istruzioni visualizzate sullo schermo per creare una nuova password.
7. Se richiesto, cliccare su **Crea nuovo portachiavi**.

Gli utenti potranno nuovamente accedere al volume di avvio del proprio computer.

Negli endpoint che eseguono macOS 10.12 o versioni precedenti, una nuova chiave verrà creata e memorizzata in Sophos Central. Una chiave di ripristino può essere adoperata una sola volta. Se dovesse essere necessario ripristinare nuovamente il computer, occorrerà recuperare una nuova chiave di ripristino.

Negli endpoint che eseguono macOS 10.13 e Apple File System (APFS), non verrà creata alcuna chiave di ripristino. La chiave di ripristino attuale continuerà a essere valida.

Attività correlate

Recupero della chiave di ripristino tramite portale self-service (pagina 22)
Se gli utenti non dovessero essere in grado di accedere ai propri computer (ad es. nel caso in cui abbiano dimenticato il PIN di BitLocker, la password di macOS, ecc.), potranno adoperare il Sophos Self Service Portal per recuperare una chiave di ripristino.

Sblocco dei volumi HFS+ mediante i comandi del Terminal (pagina 17)
È possibile utilizzare i comandi del Terminal per sbloccare volumi cifrati. I comandi indicati in questa sezione sono applicabili a endpoint che eseguono macOS 10.12 o versioni precedenti, con volumi formattati con HFS+.

Sblocco dei volumi APFS mediante i comandi del Terminal (pagina 17)
È possibile utilizzare i comandi del Terminal per sbloccare volumi cifrati. I comandi in questa sezione sono applicabili a endpoint che eseguono macOS 10.13 e Apple File System (APFS).

Informazioni correlate

Informazioni su macOS Recovery
Come selezionare un disco di avvio diverso
Guida in linea di Sophos Central

3.3.1 Sblocco dei volumi HFS+ mediante i comandi del Terminal

È possibile utilizzare i comandi del Terminal per sbloccare volumi cifrati. I comandi indicati in questa sezione sono applicabili a endpoint che eseguono macOS 10.12 o versioni precedenti, con volumi formattati con HFS+.

Queste istruzioni indicano cosa vedono gli utenti e come devono procedere. Dovranno:

1. Aprire l'applicazione **Terminal** ed eseguire `diskutil corestorage list`.
   Verrà visualizzato un elenco di tutti i volumi connessi.
2. Cercare il nome del volume (`LV Name`) da ripristinare e prendere nota dell'ID del `Logical Volume`.
3. Contattare l'amministratore e richiedere la chiave di ripristino utilizzando l'ID del `Logical Volume` come ID chiave di ripristino.
   L'amministratore fornirà la chiave di ripristino. Per assistenza durante il recupero della chiave di uno degli utenti, consultare la Guida in linea di Sophos Central.
4. Inserire la chiave di ripristino nella finestra di dialogo della password del disco per sbloccare il disco.
   In alternativa, per sbloccare il disco, gli utenti possono adoperare il comando `diskutil corestorage unlockVolume` e inserire la chiave di ripristino nell'applicazione **Terminal**.

Sarà ora possibile accedere al disco nel Finder.

Informazioni correlate

Guida in linea di Sophos Central

3.3.2 Sblocco dei volumi APFS mediante i comandi del Terminal

È possibile utilizzare i comandi del Terminal per sbloccare volumi cifrati. I comandi in questa sezione sono applicabili a endpoint che eseguono macOS 10.13 e Apple File System (APFS).

Queste istruzioni indicano cosa vedono gli utenti e come devono procedere. Dovranno:

1. Aprire l'applicazione **Terminal** ed eseguire `diskutil apfs list`.
   Verrà visualizzato un elenco di tutti i volumi connessi.
2. Cercare il nome del volume che desiderano recuperare e annotare il codice identificativo del volume, ad es: `Volume disk1s1`.
3. Contattare l'amministratore e richiedere la chiave di ripristino utilizzando il codice identificativo del volume come ID chiave di ripristino.
   L'amministratore fornirà la chiave di ripristino. Per assistenza durante il recupero della chiave di uno degli utenti, consultare la Guida in linea di Sophos Central.
4. Inserire la chiave di ripristino nella finestra di dialogo della password del disco per sbloccare il disco.
   In alternativa, per sbloccare il disco, gli utenti possono adoperare il comando `diskutil apfs unlockVolume` e inserire la chiave di ripristino nell'applicazione **Terminal**.

Sarà ora possibile accedere al disco nel Finder.

Informazioni correlate
Guida in linea di Sophos Central

3.3.3 Errore: Non è stato possibile memorizzare la chiave di ripristino

In alcune rare eventualità, è possibile che il sistema non sia in grado di memorizzare la chiave di ripristino localmente (nel portachiavi) o in Sophos Central.

Ciò significa che non sarà possibile ripristinare il computer nel caso in cui l'utente dimenticasse la password. Per mitigare questo rischio, viene visualizzato un messaggio di errore con la chiave di ripristino, e viene richiesto all'utente di effettuare una copia della chiave di ripristino.

Il sistema continuerà ripetutamente a effettuare tentativi di memorizzare la chiave di ripristino in Sophos Central. Non appena questa operazione riesca a essere completata, verrà comunicato all'utente che è ora presente una nuova chiave di ripristino gestita da Sophos Central, e che può eliminare definitivamente la propria copia della chiave di ripristino.

3.4 Stato di cifratura dei dispositivi (Mac)

Gli utenti possono accedere alle informazioni relative allo stato di cifratura con l'applicazione **Sophos Device Encryption**. È installata nella directory `Applicazioni` e può essere avviata con Finder, Launchpad o Spotlight.

L'applicazione **Sophos Device Encryption** fornisce le seguenti informazioni:

- Stato del criterio: la prima riga comunica agli utenti se un endpoint è gestito o meno con Sophos Device Encryption.
- Stato dell'utente: la seconda riga comunica agli utenti le azioni che gli utenti sono autorizzati o meno a svolgere.
- Stato del disco: viene visualizzato un elenco di tutti i dischi interni. Se il nome di un disco viene visualizzato in grigio e non è selezionabile, significa che il disco non è attualmente montato. Un'icona accanto al nome del disco ne indica lo stato. Sono disponibili i seguenti stati:
  - Verde: il disco è completamente cifrato, e la chiave di ripristino è conservata centralmente.
  - Giallo: il disco è completamente cifrato, ma la chiave di ripristino non è conservata in Sophos Central. Questa situazione può verificarsi quando Sophos Central risulta momentaneamente non raggiungibile. Se non viene richiesta la cifratura del disco, è possibile che una chiave di ripristino non esista neppure. Solitamente ciò avviene quando il disco non è gestito da Sophos Central Device Encryption ed è stato cifrato con gli strumenti del sistema operativo.
  - Giallo + punto esclamativo: il disco è cifrato per intero, è presente un criterio che richiede la cifratura del disco, ma non è disponibile alcuna chiave di ripristino.
  - Rosso: il disco non è cifrato, ma è presente un criterio che richiede la cifratura del disco.
  - Grigio: il disco non è cifrato e il criterio non richiede la cifratura, oppure non esiste alcun criterio.
  - Barra di stato + **Cifratura in corso**: È in corso la cifratura del disco.
  - Barra di stato + **Decifratura in corso**: È in corso la decifratura del disco.

Nota
Se un utente con privilegi di amministrazione su un endpoint Mac dovesse effettuare il tentativo di decifrare manualmente il proprio hard disk quando è stato applicato un criterio di cifratura, Sophos Central non potrà assumere la priorità rispetto al comando dell'utente, e il disco verrà decifrato. Una volta completata la decifratura, all'utente sarà richiesto di inserire la propria password per abilitare FileVault, e il disco verrà nuovamente cifrato.

- Stato di ripristino: Nella parte bassa della finestra, viene comunicato agli utenti se siano disponibili chiavi di ripristino per i propri dischi.

In alternativa, è possibile accedere alle informazioni sullo stato della cifratura dei dispositivi da uno strumento da riga di comando. Questo strumento è installato nel percorso `/usr/local/bin/seadmin`. Sono disponibili i seguenti comandi:

- `help`: visualizza un elenco dei comandi disponibili.
- `status`: visualizza l'ultima sincronizzazione del software di cifratura e l'intervallo di sincronizzazione.
- `--device-encryption`: visualizza il criterio di cifratura attuale, insieme allo stato di cifratura e ripristino di tutti i dischi interni.

4 Protezione dei file con password per una condivisione sicura

Questa funzionalità può essere attivata in un criterio di **Device Encryption**.

> **Nota**
> Questa funzionalità è disponibile solamente in Central Device Encryption 2.0 e versioni successive. È disponibile solo per Windows.

È possibile proteggere file con dimensioni fino a 50 MB.

Abilita menu di scelta rapida del tasto destro del mouse: attivando questa opzione, viene visualizzata un'opzione **Crea file protetto da password** nel menu del tasto destro del mouse. Gli utenti possono allegare alle e-mail file protetti con password quando vengono inviati dati di natura sensibile a destinatari situati all'esterno del perimetro di rete aziendale. I file vengono inclusi in un nuovo file HTML dal contenuto cifrato.

I destinatari possono quindi aprire il file facendo doppio clic sul file e immettendo la password. Possono inviare nuovamente il file ricevuto e proteggerlo con la stessa password o una password nuova, oppure possono creare un nuovo file protetto con password.

Abilita add-in per Outlook: Questa opzione consente di aggiungere ad Outlook la cifratura degli allegati e-mail. Gli utenti possono proteggere gli allegati selezionando la dicitura **Proteggi allegati** nella barra multifunzione di Outlook. Tutti gli allegati non protetti vengono inclusi in un nuovo allegato HTML dal contenuto cifrato, e l'e-mail viene inviata.

Chiedi sempre come procedere con i file in allegato: Se viene attivata questa opzione, gli utenti dovranno selezionare la modalità di invio degli allegati per ogni messaggio contenente allegati. Gli allegati possono essere inviati come file protetti con password, oppure senza protezione.

È possibile immettere domini esclusi, ai quali l'opzione **Chiedi sempre come procedere con i file in allegato** non è applicabile, ad esempio il dominio della propria organizzazione. Se il destinatario appartiene a questo dominio, ai mittenti non verrà richiesto di specificare la modalità di invio degli allegati.

Specificare solamente nomi di dominio completi, separati da virgole.

Informazioni correlate

Criterio di Device Encryption

5 Richiesta agli utenti di modificare la password o il PIN

Esistono due modi per richiedere agli utenti di modificare la propria password.

Nota
Questa opzione è disponibile solo per Windows.

- Utilizzare l'opzione **Richiedi agli utenti una nuova password/un nuovo PIN di autenticazione** nel criterio di cifratura.

  Questa opzione è disattivata per impostazione predefinita. Richiede la modifica obbligatoria della password o del PIN di BitLocker una volta trascorso l'intervallo di tempo specificato. Quando gli utenti modificano password o PIN, verrà creato un evento nel log.

  Nota
  Questa funzionalità è disponibile solamente in Central Device Encryption 2.0 e versioni successive.

- Utilizzare l'opzione **Attiva modifica di password/PIN** nella scheda **Riepilogo** della pagina dei dettagli di un computer.

  Questa opzione impone agli utenti di modificare immediatamente la password o il PIN di BitLocker. Una volta inviata la richiesta, verrà visualizzato un messaggio.

Sull'endpoint, verrà richiesto agli utenti di impostare una nuova password o PIN di BitLocker. Se gli utenti chiudono la finestra di dialogo senza immettere password o PIN, questa finestra verrà visualizzata nuovamente dopo 30 secondi. Il processo verrà ripetuto fino all'immissione dei dati richiesti. Se gli utenti chiudono questa finestra di dialogo cinque volte senza modificare password o PIN, verrà inserito un avviso nel log.

Informazioni correlate
Criterio di Device Encryption
Riepilogo del computer

6 Recupero della chiave di ripristino tramite portale self-service

Se gli utenti non dovessero essere in grado di accedere ai propri computer (ad es. nel caso in cui abbiano dimenticato il PIN di BitLocker, la password di macOS, ecc.), potranno adoperare il Sophos Self Service Portal per recuperare una chiave di ripristino.

Con la chiave di ripristino, potranno avere nuovamente accesso al computer.

Per consentire agli utenti di ripristinare i computer nel portale self-service, selezionare **Sophos Central > Persone > Utenti**, selezionare uno o più utenti e cliccare sul pulsante **Link di configurazione email**. Nella finestra di dialogo seguente, selezionare **Email di configurazione/ benvenuto del servizio self-service Sophos Central** per inviare agli utenti un link di attivazione via e-mail. Quando gli utenti seguono le istruzioni indicate nell'e-mail, potranno adoperare il Sophos Self Service Portal per ripristinare i propri computer.

Queste istruzioni indicano cosa vedono gli utenti e come devono procedere. Dovranno:

1. Accedere al portale self-service di Sophos con un altro computer.
2. Navigare sulla pagina **Device Encryption**.
   Viene visualizzato un elenco di tutti i computer nei quali l'utente è stato l'ultimo ad aver effettuato l'accesso. Se nel frattempo un altro utente dovesse aver effettuato l'accesso a uno dei computer, non sarà possibile ottenere nuovamente l'accesso a tale computer tramite portale self-service.
3. Selezionare un computer dall'elenco e cliccare sul pulsante **Recupera** nella colonna **CHIAVE DI RIPRISTINO**.
   Verrà visualizzata una finestra di dialogo con la chiave di ripristino.
4. Avviare il proprio computer e caricare la pagina di ripristino.
   - Windows: Premere il tasto **ESC** per passare alla schermata **Ripristino BitLocker**.
   - Mac: Cliccare sull'icona a forma di punto interrogativo nel campo **Password** per passare alla pagina di ripristino di FileVault.
5. Inserire la chiave di ripristino.

Gli utenti potranno nuovamente accedere al proprio computer.

Informazioni correlate

Portale self-service

7 Approfondimenti

Windows

- Domande frequenti: articolo 124819 della knowledge base
- Domande frequenti (FAQ) su BitLocker
- Impostazioni del criterio di gruppo per BitLocker
- I principi di base di TPM
- Impostazioni del criterio di gruppo per TPM
- Panoramica tecnica per l’amministrazione del Trusted Platform Module

Mac

- Domande frequenti: articolo 125982 della knowledge base
- Configurazione di FileVault: Uso di FileVault per codificare il disco di avvio sul Mac
- Chiavi di recupero FileVault: Impostare una chiave di recupero FileVault per i computer nel tuo istituto
- Reimposta password: Modificare o reimpostare la password di un account utente macOS

Informazioni correlate

Domande frequenti (FAQ) su BitLocker
Impostazioni del criterio di gruppo per BitLocker
Impostazioni del criterio di gruppo per TPM
I principi di base di TPM
Panoramica tecnica per l’amministrazione del Trusted Platform Module
Uso di FileVault per codificare il disco di avvio sul Mac
Impostare una chiave di recupero FileVault per i computer nel tuo istituto
Modificare o reimpostare la password di un account utente macOS
Articolo 124819 della knowledge base
Articolo 125982 della knowledge base

8 Browser web supportati

Attualmente sono supportati i seguenti browser:

- Microsoft Internet Explorer 11 e Microsoft Edge.
- Google Chrome.
- Mozilla Firefox.
- Apple Safari (solo Mac).

Si consiglia di installare o effettuare l'upgrade a una versione supportata indicata nell'elenco di cui sopra, e di eseguire sempre una versione aggiornata. Il nostro obiettivo è offrire supporto dell'ultima versione e della versione a essa precedente di Google Chrome, Mozilla Firefox e Apple Safari. Se dovesse essere rilevato un browser non supportato, si verrà reindirizzati su https://central.sophos.com/unsupported.

Nota
Sophos Central Admin non è supportata sui dispositivi mobili.

9 Ulteriore assistenza

Per ricevere assistenza dal Supporto tecnico Sophos:

1. Cliccare su **Guida** nella parte in alto a destra dell'interfaccia utente e selezionare **Crea ticket di supporto**.
2. Compilare il modulo. Si consiglia di essere quanto più precisi possibile, per consentire al Supporto tecnico di fornire un'assistenza adeguata.
3. Opzionalmente, è possibile selezionare questa opzione per permettere al Supporto tecnico di accedere direttamente alla sessione di Sophos Central, a scopo di fornire assistenza.
4. Cliccare su **Invia**.

Sophos vi contatterà entro 24 ore.

Nota
Se è stata selezionata l'opzione che consente al Supporto tecnico di accedere alla propria sessione di Sophos Central, questa funzione verrà attivata quando si clicca su **Invia**. L'assistenza remota viene disattivata automaticamente dopo 72 ore. Per disattivarla anticipatamente, cliccare sul nome dell'account (nella parte in alto a destra dell'interfaccia utente), selezionare **Dettagli account**, e cliccare sulla scheda **Supporto tecnico Sophos**.

Invio di feedback

Per inviare commenti o suggerimenti al Supporto tecnico Sophos:

1. Cliccare su **Guida** nella parte in alto a destra dell'interfaccia utente e selezionare **Invia commenti e suggerimenti**.
2. Compilare il modulo.
3. Cliccare su **Invia**.

Ulteriore assistenza

È possibile ricevere assistenza tecnica anche come segue:

- 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.

10 Note legali