

SOPHOS

simple + secure

SafeGuard Enterprise

Guida in linea

Versione prodotto: 5.60
Data documento: aprile 2011



Sommario

1	SafeGuard Enterprise su computer endpoint.....	3
2	Autenticazione all'accensione.....	3
3	Autenticazione all'accensione con Windows Vista e Windows 7.....	17
4	Accesso a Windows Vista e Windows 7.....	20
5	Accesso mediante Lenovo Fingerprint Reader.....	21
6	Opzioni di recupero.....	28
7	Recupero tramite Local Self Help.....	29
8	Recupero mediante richiesta/risposta.....	39
9	Icona dell'area di notifica e descrizione comandi.....	46
10	Accesso alle funzioni mediante estensioni di Esplora risorse.....	48
11	Cifratura dei dati.....	49
12	SafeGuard Data Exchange.....	53
13	SafeGuard Configuration Protection.....	65
14	SafeGuard Enterprise e BitLocker Drive Encryption.....	67
15	SafeGuard Enterprise e autocifratura, dischi rigidi conformi allo standard Opal.....	69
16	SafeGuard Enterprise e Lenovo Rescue and Recovery.....	69
17	Supporto tecnico.....	74
18	Note legali.....	75

1 SafeGuard Enterprise su computer endpoint

SafeGuard Enterprise è una suite di protezione modulare che applica la protezione ai PC e ai dispositivi mobili su più piattaforme mediante criteri definiti dall'amministratore. SafeGuard Enterprise è facile da utilizzare. L'amministrazione del sistema viene gestita in modo centralizzato dal SafeGuard Management Center.

Le funzioni di protezione centrali di SafeGuard Enterprise su computer endpoint sono costituite dalla cifratura dei dati e dalla protezione dagli accessi non autorizzati a un computer mediante supporti esterni.

Moduli di SafeGuard Enterprise

■ SafeGuard Enterprise Device Encryption

- Autenticazione all'accensione
- L'accesso viene eseguito immediatamente dopo l'accensione del computer. Dopo aver eseguito l'Autenticazione all'accensione, l'utente accede automaticamente al sistema operativo. Se si desidera, è possibile disattivare l'Autenticazione all'accensione. In questo caso l'autenticazione viene eseguita tramite il sistema operativo.
- Cifratura basata su volume
- Supporto BitLocker

■ SafeGuard Data Exchange

- SafeGuard Data Exchange facilita lo scambio di dati tramite supporti rimovibili su tutte le piattaforme, senza il bisogno di una nuova cifratura.
- Cifratura basata su file
- Tutti i supporti rimovibili scrivibili, inclusi i dischi rigidi esterni e gli stick USB vengono cifrati in modo trasparente.

■ SafeGuard Configuration Protection

Utilizzando SafeGuard Configuration Protection i responsabili della protezione possono consentire l'esecuzione solo di determinate interfacce o dispositivi periferici nei computer selezionati. Ciò blocca l'esposizione al malware e l'esportazione di dati tramite canali indesiderati quali ad esempio le WLAN. Questo modulo è inoltre in grado di rilevare e bloccare hardware dannosi quali i key logger.

Nota: Alcune funzionalità descritte in questo manuale possono non essere disponibili sul proprio computer. Ciò avviene in quanto le funzioni a propria disposizione dipendono dai criteri impostati dal responsabile della protezione.

2 Autenticazione all'accensione

L'autenticazione all'accensione (POA) richiede che venga eseguita l'autenticazione prima dell'avvio del sistema operativo del computer. In seguito a tale operazione, Windows viene avviato e l'accesso viene effettuato automaticamente. La procedura è identica quando il computer esce da una fase di ibernazione (Suspend to Disk).



Aspetto dell'autenticazione all'accensione

L'aspetto della schermata dell'autenticazione all'accensione può essere personalizzato in base alle esigenze della società. Il responsabile della protezione può fare ciò impostando i criteri all'interno di SafeGuard Management Center.

Sono possibili le seguenti personalizzazioni:

- **Immagine di accesso**

L'immagine di accesso predefinita visualizzata durante l'Autenticazione all'accensione è un design di SafeGuard. Questa schermata è personalizzabile mediante criteri e consente di utilizzare elementi grafici, quali, ad esempio, il logo della propria società.

- **Testo della finestra di dialogo**

Tutti i testi dell'Autenticazione all'accensione sono visualizzati nella lingua predefinita, impostata nel computer mediante le Opzioni internazionali e della lingua di Windows durante l'installazione di SafeGuard Enterprise. Eseguita l'installazione, è possibile modificare il testo della finestra di dialogo dell'autenticazione all'accensione, semplicemente cambiando la lingua predefinita nelle Opzioni internazionali e della lingua di Windows. Il responsabile della protezione può personalizzare la lingua del testo della finestra di dialogo all'interno di un criterio.

2.1 Primo accesso dopo l'installazione di SafeGuard Enterprise

Se SafeGuard Enterprise è stato installato con l'autenticazione all'accensione (POA), la procedura di avvio sarà diversa al primo avvio del sistema dopo l'installazione di SafeGuard Enterprise. Verranno visualizzati alcuni nuovi messaggi di avvio (ad esempio la schermata di accesso automatico), in quanto SafeGuard Enterprise è stato incorporato nella procedura di avvio. Successivamente sarà avviato il sistema operativo Windows.

Al primo accesso dopo l'installazione, è necessario accedere prima a Windows correttamente, come di consueto. Dopo aver portato a termine questa operazione, si verrà registrati come utenti di SafeGuard Enterprise. Il processo di registrazione è necessario per garantire il riconoscimento delle credenziali dell'utente durante l'autenticazione all'accensione al successivo avvio del sistema.

Nota: Una volta effettuata la registrazione e ricevuti tutti i dati richiesti, verrà visualizzata una notifica del completamento del processo.

Al riavvio del computer viene attivata l'autenticazione all'accensione. D'ora in avanti, per l'Autenticazione all'accensione, dovranno essere inserite le credenziali Windows. L'accesso a Windows viene quindi eseguito automaticamente senza l'ulteriore inserimento di una password (se l'accesso automatico a Windows è attivato).

È possibile accedere all'Autenticazione all'accensione tramite:

- nome utente e password
- token/smartcard e PIN

Per i dispositivi più aggiornati supportati, consultare le note di rilascio.

Nota: Le impostazioni per i computer endpoint nei quali è installato SafeGuard Enterprise vengono definite dal responsabile della protezione in SafeGuard Management Center, e distribuite agli utenti tramite file di criteri.

Procedura di primo accesso

Il primo accesso corrisponde a quanto descritto in questa sezione, soltanto se sul computer è stata installata e attivata l'Autenticazione all'accensione.

A seconda della configurazione del sistema, è possibile che venga richiesto di premere **Ctrl+Alt+Canc**. In seguito, il processo di avvio continua.

2.1.1 Accesso automatico a SafeGuard

All'avvio del computer viene visualizzata la finestra di dialogo dell'**Accesso automatico a SafeGuard**.

Cosa succede?

1. Un utente ha effettuato l'accesso automatico.
2. Se è presente una connessione a SafeGuard Enterprise Server, il computer viene automaticamente registrato al SafeGuard Enterprise Server.
3. La chiave del computer viene inviata al SafeGuard Enterprise Server e memorizzata nel database di SafeGuard Enterprise.
4. I criteri del computer vengono inviati al computer.

2.1.2 Accesso a Windows

Verrà visualizzata la finestra di dialogo di accesso a Windows.

Immettere le proprie credenziali di Windows, come di consueto.

Nota: Se si utilizza una **smartcard** o un **token**, immettere il PIN.

Cosa succede?

1. L'ID utente e un hash delle credenziali vengono inviati al server.

2. I criteri utente, i certificati e le chiavi vengono creati e inviati al computer endpoint.

I dati relativi all'utente saranno disponibili all'Autenticazione all'accensione soltanto dopo essere stati sincronizzati tra il server SafeGuard Enterprise e il computer endpoint.

Nota: Una volta effettuata la registrazione e ricevuti tutti i dati richiesti, viene visualizzata una notifica di conferma del processo.

Al successivo avvio del sistema sarà sufficiente immettere una le proprie credenziali Windows (nome utente e password) durante l'Autenticazione all'accensione. L'accesso a Windows viene effettuato automaticamente.

Per attivare pienamente l'Autenticazione all'accensione è necessario riavviare il sistema. Una volta riavviato il computer, l'Autenticazione all'accensione proteggerà il computer dagli accessi non autorizzati.

2.1.3 Autenticazione all'accensione dopo il riavvio del computer

Dopo aver riavviato il computer viene visualizzata la finestra di dialogo dell'Autenticazione all'accensione.

Inserire nome utente e password.

Cosa succede?

1. Le credenziali vengono valutate. Vengono messi a disposizione i certificati e le chiavi e viene eseguito automaticamente l'accesso a Windows.

Nota: L'accesso pass-through a Windows può essere disattivata tramite un criterio. In questo caso viene visualizzata la finestra di dialogo di accesso a Windows e sarà necessario inserire le proprie credenziali.

2.2 Accesso mediante autenticazione all'accensione

Dopo aver attivato l'autenticazione all'accensione (POA), l'accesso viene effettuato immettendo le proprie credenziali utente di Windows nella finestra di dialogo di accesso a POA. L'accesso a Windows viene effettuato automaticamente.

Nota:

È possibile disattivare l'accesso automatico a Windows cliccando sul pulsante **Opzioni >>** nella finestra di dialogo di accesso e disattivando l'opzione **Accesso pass-through a Windows**. Ad esempio, è necessario disattivare l'accesso automatico per consentire ad altri utenti di utilizzare l'autenticazione all'accesso sullo stesso computer (*vedere Importazione di altri utenti* a pagina 7).

Quando si accede a POA, assicurarsi di distinguere tra maiuscole e minuscole.

Ritardo di accesso nel caso di tentativo di accesso non riuscito

Se l'accesso all'autenticazione all'accensione non riesce, ad esempio in seguito ad un errore di digitazione della password, viene visualizzato un messaggio di errore ed entra in vigore un ritardo di accesso per il successivo tentativo. Il tempo di attesa viene incrementato ad ogni tentativo di accesso non riuscito. I tentativi non riusciti vengono registrati nel log.

Blocco del computer

A seconda delle impostazioni dei criteri, il computer può venire bloccato in seguito ad un determinato numero di tentativi di accesso non riusciti. Per sbloccare il computer, avviare una procedura di richiesta/risposta, [vedere Recupero mediante richiesta/risposta](#) a pagina 39.

2.2.1 Recupero dell'accesso

Nel caso di recupero dell'accesso, se, per esempio, si è dimenticata la password, SafeGuard Enterprise offre diverse opzioni, ciascuna adeguata a un determinata situazione di recupero. I metodi di recupero disponibili per il proprio computer dipendono dalle impostazioni scelte dal responsabile della protezione. Per ulteriori informazioni, [vedere Opzioni di recupero](#) a pagina 28.

2.3 Importazione di altri utenti

Per consentire l'accesso al computer da parte di un altro utente di Windows:

1. Accendere il computer.

Viene visualizzata la finestra dell'Autenticazione all'accensione. Il secondo utente di Windows non può accedere all'Autenticazione all'accensione, poiché non dispone delle chiavi e dei certificati necessari.

2. Perché il secondo utente possa accedere all'Autenticazione all'accensione, il proprietario del computer deve concedere tale permesso.

Nota: Per impostazione predefinita, il primo utente a effettuare l'accesso dopo l'installazione viene registrato come proprietario del computer. Anche il responsabile della protezione può definire il proprietario di un computer tramite l'impostazione di un criterio.

3. Nella finestra di dialogo di accesso dell'Autenticazione all'accensione, cliccare su **Opzioni** e deselezionare la casella di spunta **Pass-through a Windows**.

Verrà visualizzata la finestra di dialogo di accesso a Windows.

4. Il secondo utente inserisce le proprie credenziali Windows.
5. Se nel computer sono presenti il certificato e la chiave per il secondo utente (come indicato nel fumetto di notifica), viene creata una voce per il secondo utente all'interno del sistema di SafeGuard Enterprise.

Al successivo avvio del computer, il secondo utente potrà accedere mediante l'Autenticazione all'accensione.

Nota: Se gli utenti hanno già eseguito l'accesso mediante l'Autenticazione all'accensione in un altro computer presente nell'ambiente, il responsabile della protezione potrà utilizzare SafeGuard Management Center per assegnare gli utenti all'Autenticazione all'accensione su un nuovo computer. Gli utenti così assegnati possono accedere ai relativi computer tramite l'Autenticazione all'accensione.

2.4 Password temporanea nell'Autenticazione all'accensione

SafeGuard Enterprise consente di modificare temporaneamente la password durante l'Autenticazione all'accensione. Si consiglia la modifica della password temporaneamente, se si sospetta di essere stati osservati mentre si digitava la password.

Esempio: L'utente avvia il proprio computer portatile in un luogo pubblico, quale l'aeroporto. Si pensa di essere stati osservati durante l'inserimento della password durante l'Autenticazione all'accensione. Poiché non si è connessi ad Active Directory (AD), non è possibile modificare la password di Windows.

Soluzione: Modificare temporaneamente la password dell'Autenticazione all'accensione, in modo tale che nessun utente non autorizzato ne venga a conoscenza. Non appena ci si riconnette ad AD, verrà automaticamente richiesto di modificare la password temporanea.

1. Nella finestra di dialogo dell'Autenticazione all'accensione inserire la password in uso.
2. Premere **F8**.

Nota: Se non si inserisce la password corrente prima di premere **F8**, l'operazione verrà interpretata dal sistema come accesso errato e verrà visualizzato un messaggio d'errore.

3. Nella finestra di dialogo, inserire la nuova password e confermarla.

Un messaggio del sistema ricorda che la modifica della password è soltanto temporanea.

4. Cliccare su **OK**.

Nota: Se si annulla questa finestra di dialogo, l'accesso verrà eseguito con la password precedente.

Verrà visualizzata la finestra di dialogo di accesso a Windows.

Nota:

L'accesso non verrà eseguito tramite l'opzione pass-through di Windows, anche se il sistema è configurato in tal senso. Inserire qui la "password precedente". La password temporanea è valida soltanto per l'accesso all'autenticazione all'accensione.

5. Cliccare su **OK**.

L'utente è ora connesso a Windows.

Per accedere all'autenticazione all'accensione, è adesso possibile utilizzare la password temporanea. La password temporanea è valida soltanto fino a quando essa non verrà modificata durante l'accesso a Windows. Solo dopo avere eseguito questa operazione, sarà possibile effettuare un accesso pass-through dall'Autenticazione all'accensione a Windows.

Modifica della password temporanea

La password modificata temporaneamente durante l'autenticazione all'accensione deve essere modificata in un secondo momento, al fine di sincronizzare nuovamente le password.

Quando si accede a Windows, in SafeGuard Enterprise viene richiesto automaticamente di modificare la password non appena ci si connette nuovamente ad Active Directory.

La finestra di dialogo con la richiesta di modifica della password può essere annullata senza modificare la password. In questo caso, la finestra di dialogo viene visualizzata ogni volta che si effettua l'accesso fino a quando la password non verrà modificata.

Nota: La password per l'autenticazione all'accensione può essere modificata temporaneamente anche mentre si è connessi ad Active Directory. In questo caso, la finestra di dialogo per la modifica della password viene visualizzata immediatamente dopo la modifica temporanea della password durante l'autenticazione all'accensione. È tuttavia possibile annullare l'operazione e utilizzare la "password precedente" per l'accesso. La password potrà quindi essere modificata in un secondo momento.

2.5 Accesso mediante l'Autenticazione all'accensione utilizzando smartcard o token

Esistono due possibili tipi di accesso con smartcard o token:

- *consentito unicamente mediante smartcard o token*
- *sia tramite l'immissione di nome utente e password che mediante smartcard o token*

Il responsabile della protezione definisce in modo centralizzato il tipo di accesso consentito impostando un criterio appropriato.

Il responsabile della sicurezza emette la smartcard o il token e lo fornisce all'utente. L'utente può inserire personalmente le credenziali utente di Windows nella propria smartcard o token.

Nota: In SafeGuard Enterprise le smartcard e i token vengono gestiti allo stesso modo. Di conseguenza i termini "token" e "smartcard" sono la medesima cosa sia nel prodotto che nel manuale. Nelle seguenti sezioni viene utilizzato il termine token.

2.5.1 Primo accesso con token dopo l'installazione

Il primo accesso effettuato con token è identico alla procedura per l'accesso senza token.

Se si dispone di un token, è possibile utilizzarlo per accedere a Windows immettendo il relativo PIN.

Nota: Si consiglia di configurare il token con le proprie credenziali utente di Windows ([vedere Memorizzazione delle credenziali utente Windows nel token](#) a pagina 10), prima di eseguire il riavvio del computer. I criteri di protezione applicati all'utente potrebbero richiedere l'utilizzo di un token al momento dell'Autenticazione all'accensione. Se il token non contiene le credenziali dell'utente, non sarà possibile accedere tramite l'Autenticazione all'accensione.

2.5.2 Accesso tramite Autenticazione all'accensione con token

Prerequisiti: Assicurarsi che nel BIOS sia attivato il supporto USB. Il supporto del token deve essere stato inizializzato e il token emesso.

1. Inserire il token.

2. Accendere il computer.

Viene visualizzata la finestra di dialogo di accesso con token.

Nota: Se il criterio applicato consente di accedere con le proprie credenziali utente e si disconnette il token, per accedere al computer sarà necessario inserire le proprie credenziali. Se la finestra di dialogo per l'accesso con ID utente e password non viene visualizzata, è possibile accedere solo tramite l'Autenticazione all'accensione utilizzando un token.

3. Inserire il PIN del token.

L'accesso viene effettuato mediante l'Autenticazione all'accensione e l'accesso a Windows (se la casella di spunta **Pass-through a Windows** è selezionata nella finestra di dialogo di accesso).

2.5.3 Modifica del PIN

È possibile modificare il PIN del token dalla finestra di dialogo di accesso.

Se al momento dell'Autenticazione all'accensione (POA) è attivata l'opzione **Pass through a Windows**, la finestra di dialogo di accesso a Windows non viene di solito visualizzata. Per visualizzarla, è necessario disattivare questa opzione durante l'accesso all'Autenticazione all'accensione.

Nota: Se il responsabile della protezione ha definito delle regole che richiedono la modifica del PIN, verrà richiesto automaticamente di eseguire tale modifica (ad esempio, a intervalli regolari).

1. Nella finestra di dialogo **PIN** per l'accesso a Windows, selezionare la casella di spunta **Modifica PIN**.
2. Inserire il PIN del token e cliccare su **OK**.

Viene visualizzata la finestra di dialogo **Modifica PIN**.

3. Immettere il nuovo PIN e confermarlo.
4. Cliccare su **OK**.

Il PIN del token viene modificato e la procedura di accesso a Windows continua.

2.5.4 Memorizzazione delle credenziali utente Windows nel token

Se il token non contiene le credenziali utente di Windows, è possibile memorizzarle nel token autonomamente.

Nota: Si consiglia di configurare il token durante il primo accesso. I criteri di protezione applicati all'utente potrebbero richiedere l'utilizzo di un token al momento dell'Autenticazione all'accensione. Se il token non contiene informazioni sull'utente, non sarà possibile accedere mediante l'Autenticazione all'accensione.

1. Durante il primo accesso dopo l'installazione, collegare il token al sistema quando viene visualizzata la finestra di dialogo di accesso a Windows.

Se il sistema rileva un token vuoto, viene automaticamente visualizzata la finestra di dialogo **Emissione token**.

2. Inserire nome utente e password di Windows.
3. Confermare la password.
4. Selezionare o inserir il dominio e cliccare su **OK**.

Il sistema tenta di accedere a Windows utilizzando i dati inseriti. Se l'accesso riesce, i dati vengono scritti nel token.

L'utente è ora connesso a Windows.

Se l'accesso con token è definito come opzione facoltativa per l'utente (l'utente ha già effettuato l'accesso mediante l'Autenticazione all'accensione con il proprio nome utente e password), è possibile anche emettere il token in un secondo momento.

Per far ciò, nella finestra di dialogo di accesso dell'Autenticazione all'accensione, cliccare su **Opzioni** e deselezionare la casella di spunta **Pass-through a Windows**. Viene visualizzata la finestra di dialogo di accesso a Windows e sarà possibile memorizzare i dati nel token come descritto.

2.5.5 Recupero dell'accesso tramite token

Se si utilizza un token non di cifratura e si è dimenticata il PIN, è possibile recuperare l'accesso al computer tramite uno dei seguenti metodi di recupero:

- Recupero tramite Local Self Help, [vedere Recupero tramite Local Self Help](#) a pagina 29.
- Recupero tramite Challenge/Response, [vedere Recupero mediante richiesta/risposta](#) a pagina 39.

I metodi di recupero disponibili per il proprio computer dipendono dalle impostazioni scelte dal responsabile della protezione.

Per dare inizio al recupero, cliccare sul pulsante **Recupero** nella finestra di dialogo relativa all'accesso mediante token.

Nota:

Questi metodi di recupero non sono disponibili per i token di cifratura. Se si verificano problemi di accesso, contattare il responsabile della protezione.

2.5.6 Sblocco token

Se viene inserito più volte un PIN non corretto, il token viene bloccato. Il responsabile della protezione può configurare SafeGuard Enterprise in modo che venga visualizzata la finestra di dialogo **Sblocco token**:

Il responsabile della protezione deve fornire all'utente il PIN di amministratore definito nel token.

1. Nella finestra di dialogo **Sblocco token**, inserire il PIN di amministratore.
2. Inserire un nuovo PIN e confermarlo.

Il PIN inserito è soggetto alle regole definite per i PIN (ad esempio potrebbero essere richieste determinate combinazioni di caratteri, l'uso di PIN già utilizzati potrebbe essere vietato e così via).

3. Cliccare su **OK**.

Il token viene sbloccato e la procedura di accesso continua.

Nota:

Se questa funzione non è disponibile nel computer, è possibile tornare ad accedere al computer tramite la procedura Challenge/Response. Tramite la procedura Challenge/Response è possibile accedere nuovamente al computer, ma non è possibile cambiare il PIN o le credenziali utente.

2.5.7 Connessione desktop remoto

In Windows XP, non è possibile stabilire una connessione desktop remoto, nel caso in cui l'utente abbia effettuato l'accesso localmente mediante un token.

L'Acquisizione remota non è disponibile in questo caso.

2.5.8 Token di cifratura - Kerberos

Se si utilizzano token di cifratura, l'autenticazione viene eseguita durante la PUA, tramite il certificato memorizzato presente nel token.

Per questo tipo di accesso è necessario un token pienamente emesso. Il token deve essere fornito dal responsabile della protezione o da un'altra persona autorizzata. Per accedere al sistema, è sufficiente inserire il PIN del token. Se questo è l'unico tipo di accesso valido per il computer, non sarà possibile effettuare l'accesso senza il token.

Nota: Se si utilizzano token di questo tipo, né la procedura Challenge/Response né il Local Self Help sono disponibili nel caso di problemi di accesso. Se si verificano problemi di accesso, contattare il responsabile della protezione.

2.5.8.1 Modifica del certificato per l'accesso con token di cifratura

Per modificare o rinnovare un certificato utilizzato per eseguire l'accesso con token di cifratura, il responsabile della protezione può assegnare un nuovo certificato al computer. Una volta eseguita la sincronizzazione tra il computer e SafeGuard Enterprise Server, la finestra di stato visualizzata cliccando sull'icona nell'area di notifica di SafeGuard Enterprise indica che il computer è **Pronto per la modifica del certificato**.

Il responsabile della protezione fornisce il nuovo token.

Per modificare il certificato nel computer:

1. Accedere tramite l'Autenticazione all'accensione utilizzando il token precedente e senza accedere automaticamente a Windows.

Cliccare su **Opzioni** e deselezionare la casella di spunta **Pass through a Windows**, oppure disconnettersi di nuovo, una volta eseguito l'accesso automatico a Windows.

2. Accedere a Windows con il nuovo token.

Il nuovo token è valido per l'accesso tramite POA. Il token non è più valido per l'accesso.

2.6 Accesso automatico all'Autenticazione all'accensione tramite smartcard o token

Prerequisiti:

- Assicurarsi che nel BIOS sia attivato il supporto USB.
- Il supporto del token deve essere stato inizializzato e il token emesso.
- Il responsabile della protezione ha assegnato il relativo criterio al computer.

Se al computer è stato assegnato un criterio corrispondente a un determinato PIN predefinito, è possibile accedere automaticamente all'Autenticazione all'accensione tramite l'utilizzo di un token. Non è necessario immettere né le credenziali né il PIN, poiché questo avviene tramite l'Autenticazione all'accensione. A seconda delle impostazioni del criterio, è possibile che ciò avvenga tramite Windows.

Per eseguire l'accesso automatico tramite l'Autenticazione all'accensione utilizzando un token:

1. Inserire il token.
2. Accendere il computer.

L'utente verrà connesso automaticamente al momento dell'Autenticazione all'accensione. A seconda delle impostazioni del criterio, è possibile che ciò avvenga tramite Windows.

- Se l'accesso automatico è stato eseguito correttamente, Windows viene avviato.
- Se l'accesso automatico non viene eseguito, viene richiesto di immettere il PIN del token. L'utente verrà quindi connesso al momento dell'Autenticazione all'accensione.

2.7 Tastiera virtuale

Durante l'Autenticazione all'accensione, è possibile visualizzare/nascondere una tastiera virtuale e cliccare sui tasti sullo schermo per immettere le credenziali ed effettuare altre operazioni.

Prerequisito: Il responsabile della protezione ha abilitato la visualizzazione della tastiera virtuale nel criterio.

Per visualizzare la tastiera virtuale nell'Autenticazione all'accensione, cliccare su **Opzioni** >> nella finestra di accesso dell'Autenticazione all'accensione e selezionare la casella di spunta **Tastiera virtuale**.

La tastiera virtuale supporta layout differenti che è possibile modificare mediante le stesse opzioni utilizzate per la modifica del layout di tastiera nell'Autenticazione all'accensione ([vedere Modifica del layout di tastiera](#) a pagina 14).

2.8 Layout di tastiera

Quasi tutti i paesi hanno il proprio layout di tastiera. Il layout di tastiera nell'autenticazione all'accensione è importante per l'immissione di nomi utente, password e codici di risposta.

Per impostazione predefinita, SafeGuard Enterprise adotta il layout di tastiera delle Opzioni internazionali e della lingua per l'utente predefinito di Windows in vigore durante l'installazione di SafeGuard Enterprise.

La lingua del layout di tastiera utilizzato viene visualizzata nell'autenticazione all'accensione, ad esempio, "EN" per l'inglese. Oltre al layout di tastiera predefinito, è possibile utilizzare anche il layout di tastiera statunitense (inglese).

2.8.1 Modifica del layout di tastiera

Il layout di tastiera dell'autenticazione all'accensione (incluso il layout di tastiera virtuale) può essere modificato.

1. Selezionare **Start > Pannello di controllo > Opzioni internazionali e della lingua > Avanzate**
2. Nella scheda **Opzioni internazionali**, selezionare la lingua desiderata.
3. Nella scheda **Avanzate**, in **Impostazioni account utente predefinito**, selezionare **Applica tutte le impostazioni all'account utente corrente e al profilo utente predefinito**.
4. Cliccare su **OK**.

L'Autenticazione all'accensione riconosce il layout di tastiera utilizzato per l'ultimo accesso riuscito e lo riabilita automaticamente per quello successivo. Questa operazione richiede il doppio riavvio del computer endpoint. Se il layout di tastiera precedente viene deselezionato tramite **Opzioni internazionali e della lingua**, verrà comunque conservato fino a quando non ne venga selezionato uno diverso.

Nota:

Occorre inoltre modificare la lingua del layout di tastiera per i programmi non Unicode.

Se la lingua desiderata non è disponibile sul sistema, è possibile che Windows richieda di installarla. Una volta completata questa operazione, è necessario riavviare il computer due volte: una prima volta per consentire all'Autenticazione all'accensione di riconoscere il nuovo layout di tastiera, la seconda affinché possa impostarlo.

È possibile modificare il layout di tastiera richiesto per l'Autenticazione all'accensione con il mouse oppure con la tastiera (**Alt+Maiusc**).

Per controllare le lingue installate e disponibili sul proprio sistema, selezionare **Start>Esegui>regedit: HKEY_USERS\DEFAULT\Keyboard Layout\Preload**.

2.9 Tasti di scelta/tasti funzione supportati nell'autenticazione all'accensione

Alcune impostazioni e funzionalità hardware possono generare problemi durante l'avvio del computer, causando l'interruzione del sistema. L'Autenticazione all'accensione supporta una

varietà di tasti di scelta per modificare le impostazioni hardware e disattivare tali funzionalità. Inoltre, nel file .msi installato nel computer è integrata una gray list contenente una serie di funzionalità e impostazioni hardware che possono causare questo tipo di problemi.

Si consiglia di installare una versione aggiornata del file di configurazione di POA, prima di eseguire qualsiasi distribuzione di rilievo di SafeGuard Enterprise. Il file di configurazione viene aggiornato mensilmente ed è possibile scaricarlo da qui:

<ftp://POACFG:POACFG@ftp.ou.utimaco.de>

È possibile personalizzarlo in modo che rispecchi le caratteristiche dell'hardware di un particolare ambiente.

Nota:

Una volta definito un file personalizzato, tale file verrà eseguito al posto di quello già integrato nel file .msi. Soltanto nel caso in cui non sia stato definito o trovato alcun file di configurazione di POA verrà applicato quello predefinito.

Per installare il file di configurazione di POA, inserire il seguente comando:

MSIEXEC /i <pacchetto client MSI> POACFG=<percorso file di configurazione dell'autenticazione all'accensione>

Per ulteriori informazioni consultare l'articolo della knowledge base in inglese:

<http://www.sophos.com/support/knowledgebase/article/65700.html>.

L'autenticazione all'accensione supporta inoltre un certo numero di tasti funzione.

2.9.1 Tasti di scelta

Maiusc - F3 = Supporto USB Legacy (on/off)

Maiusc - F4 = Modalità grafica VESA (on/off)

Maiusc - F5 = USB 1.X e supporto 2.0 (on/off)

Maiusc - F6 = Controller ATA (on/off)

Maiusc - F7 = Solo supporto USB 2.0 (off/on); USB 1.x il supporto USB 1.x rimane impostato come da **Shift - F5**.

Maiusc - F9 = ACPI/APIC (off/on)

Matrice di dipendenza dei tasti di scelta

Maiusc - F3	Maiusc - F5	Maiusc - F7	Legacy	USB 1.x	USB 2.0	Commento
off	off	off	on	on	on	3.
on	off	off	off	on	on	Predefinito
off	on	off	on	off	off	1., 2.
on	on	off	on	off	off	1., 2.
off	off	on	on	on	off	3.

Maiusc - F3	Maiusc - F5	Maiusc - F7	Legacy	USB 1.x	USB 2.0	Commento
on	off	on	off	on	off	
off	on	on	on	off	off	
on	on	on	on	off	off	2.

1. **Maiusc - F5** disabilita USB 1.x e USB2.0.

Nota: Se si preme **Maiusc - F5** durante l'avvio, è possibile ridurre in modo considerevole il tempo di avvio dell'autenticazione all'accensione. Tuttavia, se il computer dispone di tastiera o mouse USB, è probabile che questi vengano disattivati quando si preme **Maiusc - F5**.

L'Autenticazione all'accensione può utilizzare la tastiera USB mediante BIOS SMM. Non è presente alcun supporto token USB.

- Se non è attivo alcun supporto USB, l'autenticazione all'accensione tenta di utilizzare BIOS SMM invece di effettuare il backup e il ripristino del controller USB. In questa situazione, la modalità legacy può rappresentare una soluzione.
- Supporto Legacy attivo, USB attivo. L'autenticazione all'accensione tenta di eseguire il backup e il ripristino del controller USB. A seconda della versione BIOS utilizzata, il sistema può bloccarsi.

Nota: È possibile che le modifiche apportate utilizzando i tasti di scelta siano già state specificate durante l'installazione del client di SafeGuard Enterprise Client mediante un file .mst.

Quando si modificano le impostazioni hardware tramite i tasti di scelta nell'autenticazione all'accensione, viene visualizzata una finestra di dialogo che richiede di salvare le impostazioni. Nella finestra viene visualizzato un riepilogo della configurazione che verrà salvata. Per salvare le modifiche apportate, fare clic su **Si**. Al riavvio del computer, vengono attivate le nuove impostazioni. Se si seleziona **No**, le modifiche non vengono salvate e la configurazione precedente rimane attiva anche dopo aver riavviato il computer.

Premendo **F5** in una delle finestre di dialogo dell'Autenticazione all'accensione, è possibile visualizzare un'altra finestra che indica la configurazione dei tasti di scelta utilizzata per avviare l'autenticazione all'accensione. Se i tasti di scelta sono stati modificati durante il processo di avvio, lo stato dei relativi tasti viene indicato in blu. Il blu indica che il tasto è stato utilizzato per l'avvio dell'autenticazione all'accensione, ma non ancora salvato. I valori rimasti invariati vengono visualizzati in nero. Per chiudere la finestra di dialogo, premere nuovamente **F5**, oppure **Invio**.

2.9.2 Tasti funzione nella finestra di dialogo di accesso

Nota: I tasti funzione non sono tasti di scelta.

F2 = abbandona accesso automatico.

F5 = visualizza una finestra di dialogo che indica la configurazione dei tasti di scelta utilizzata per avviare l'Autenticazione all'accensione.

F8 = modifica password nell'Autenticazione all'accensione. Utilizzare al posto del tasto **Invio** per attivare la modifica della password nell'autenticazione all'accensione dopo aver effettuato l'accesso.

Alt+Maiusc (tasti **Alt** di sinistra e **Maiusc** di sinistra) = modifica lingua di input da tedesco a inglese (o viceversa).

Annullamento e preparazione dell'autenticazione all'accensione per l'arresto del sistema.

Ctrl+Alt+Canc = in caso di autenticazione non riuscita consente di chiudere la sessione in modo sicuro. Questa combinazione di tasti ha la medesima funzione del pulsante **Arresta il sistema**.

Nota: Se l'accesso con impronta digitale è attivato, è possibile utilizzare **Ctrl+Alt+Canc** per modificare la finestra di dialogo dell'autenticazione all'accensione, ed effettuare l'accesso mediante nome utente e password. Per ulteriori informazioni, [vedere Accesso mediante Lenovo Fingerprint Reader](#) a pagina 21.

2.10 Sincronizzazione della password

SafeGuard Enterprise rileva automaticamente se la password di Windows è stata modificata e dunque non corrisponde più a quella memorizzata nel database di SafeGuard Enterprise. Questa situazione si può verificare quando si modifica la password di Windows mediante una rete VPN, su un altro computer, o in Active Directory.

Se SafeGuard Enterprise rileva questo tipo di problema viene richiesto l'inserimento della password precedente. Successivamente, la password memorizzata da SafeGuard Enterprise viene aggiornata con la nuova password di Windows.

La sincronizzazione password avviene in due situazioni:

- Durante l'accesso
- Durante una procedura di blocco/sblocco di Windows.

3 Autenticazione all'accensione con Windows Vista e Windows 7

L'Autenticazione all'accensione per Windows Vista e Windows 7 ha lo stesso aspetto e comportamento di quella per Windows XP. Sono riscontrabili differenze soltanto durante l'accesso al sistema operativo.

Nota: In questa sezione vengono descritte esclusivamente le differenze relative a Windows Vista e Windows 7. Se non vengono esplicitamente evidenziate disparità, significa che sono applicabili le procedure e i processi descritti nella sezione [vedere Autenticazione all'accensione](#) a pagina 3.

3.1 Primo accesso dopo l'installazione di SafeGuard Enterprise su Windows Vista e Windows 7

Se SafeGuard Enterprise è stato installato con l'autenticazione all'accensione, la procedura di avvio sarà diversa al primo avvio del sistema dopo l'installazione di SafeGuard Enterprise.

Verranno visualizzati alcuni nuovi messaggi di avvio (ad esempio la schermata di accesso automatico), in quanto SafeGuard Enterprise è stato incorporato nella procedura di avvio. Successivamente sarà avviato il sistema operativo Windows.

Nota: In Windows Vista e Windows 7, è prima necessario premere **Ctrl + Alt + Del** per avviare l'accesso automatico e quello standard. L'amministratore può disattivare questa impostazione nella console MMC, all'interno dell'editor oggetti criteri di gruppo, sotto **Impostazioni di Windows > Impostazioni di protezione > Criteri locali > Disattiva opzioni di protezione** (per l'accesso interattivo non è richiesto **Ctrl + Alt + Del**).

SafeGuard Enterprise esegue l'accesso basato su certificati. Pertanto, per accedere mediante l'Autenticazione all'accensione, gli utenti necessitano di chiavi e certificati. Tuttavia, le chiavi e i certificati specifici dell'utente possono essere creati soltanto dopo aver effettuato un accesso a Windows,

Al primo accesso dopo l'installazione, è, per prima cosa, necessario accedere a Windows correttamente utilizzando le proprie credenziali, come di consueto. Dopo aver portato a termine questa operazione, si verrà registrati come utenti di SafeGuard Enterprise. Il processo di registrazione è necessario per garantire il riconoscimento delle credenziali dell'utente durante l'autenticazione all'accensione al successivo avvio del sistema.

Una volta effettuata la registrazione e ricevuti tutti i dati richiesti, viene visualizzata una notifica del completamento del processo.

Al riavvio del computer viene attivata l'autenticazione all'accensione. D'ora in avanti, per l'Autenticazione all'accensione, dovranno essere inserite le credenziali Windows. L'accesso a Windows viene quindi eseguito automaticamente senza l'ulteriore inserimento di una password (se l'accesso automatico a Windows è attivato).

È possibile accedere all'Autenticazione all'accensione immettendo nome utente e password.

Nota: Le impostazioni per i computer nei quali è installato SafeGuard Enterprise sono definite in modo centralizzato dal responsabile della protezione nel SafeGuard Management Center e distribuite ai computer endpoint tramite file dei criteri.

Procedura di primo accesso

In questa sezione viene descritta la procedura di primo accesso al computer dopo l'installazione di SafeGuard Enterprise. Questa procedura corrisponderà a quella descritta, soltanto se l'Autenticazione all'accensione è stata installata e attivata sul computer.

3.1.1 Accesso automatico a SafeGuard

1. All'avvio del computer viene visualizzata la finestra di dialogo dell'Accesso automatico di SafeGuard.
 - Un utente ha effettuato l'accesso automatico.
 - Se è presente una connessione a SafeGuard Enterprise Server, il computer viene automaticamente registrato al SafeGuard Enterprise Server.
 - La chiave del computer viene inviata al SafeGuard Enterprise Server e memorizzata nel database di SafeGuard Enterprise.
 - I criteri del computer vengono inviati al computer.

3.1.2 Accesso a Windows Vista/Windows 7

1. Viene visualizzata la finestra di dialogo di accesso a Windows Vista/Windows 7.
2. In Windows Vista e Windows 7, SafeGuard Enterprise offre il metodo di autenticazione di SafeGuard Enterprise e Windows Vista/Windows 7. Windows Vista e Windows 7 forniscono due icone per ciascun metodo di autenticazione:
 - Cliccare su **Altro utente** per aprire una finestra di dialogo per l'inserimento delle credenziali.
 - Cliccare sulla seconda icona (sotto la quale è già visualizzato un nome utente) per aprire una finestra di dialogo contenente le informazioni relative all'ultimo utente che ha effettuato l'accesso al sistema. È necessario immettere soltanto la password.
3. Immettere le proprie credenziali di Windows, come di consueto.
 - L'ID utente e un hash delle credenziali vengono inviati al server.
 - I criteri utente, i certificati e le chiavi vengono creati e inviati al computer endpoint.

I dettagli relativi all'utente sono disponibili nell'Autenticazione all'accensione soltanto dopo che è avvenuta la sincronizzazione di tutti i dati tra il server di SafeGuard Enterprise e il computer dell'utente.

Questo significa che **al successivo avvio del sistema** sarà sufficiente immettere le proprie credenziali Windows (nome utente e password) durante l'Autenticazione all'accensione e l'accesso verrà effettuato automaticamente.

Per attivare completamente l'Autenticazione all'accensione è necessario riavviare il computer. Una volta riavviato il computer, l'Autenticazione all'accensione proteggerà il computer dagli accessi non autorizzati.

3.1.3 Autenticazione all'accensione dopo il riavvio del computer

1. Dopo aver riavviato il computer viene visualizzata la finestra di dialogo dell'Autenticazione all'accensione.

I certificati e le chiavi sono disponibili ed è possibile effettuare l'accesso tramite l'Autenticazione all'accensione utilizzando le proprie credenziali utente Windows.
2. Inserire il nome utente e la password e cliccare su **OK**.

Le credenziali utente vengono valutate. Dopo che il sistema ha verificato le credenziali, l'accesso a Windows viene effettuato automaticamente.

Nota: L'accesso pass-through a Windows può essere disattivata mediante l'impostazione di un criterio. In questo caso viene visualizzata la finestra di dialogo di accesso a Windows e sarà necessario inserire le proprie credenziali.

3.2 Accesso mediante autenticazione all'accensione in Windows Vista e Windows 7

Dopo aver attivato l'autenticazione all'accensione (sincronizzazione iniziale e riavvio), l'accesso viene effettuato immettendo le proprie credenziali utente di Windows nella finestra di dialogo di accesso all'autenticazione all'accensione. L'accesso a Windows viene effettuato automaticamente.

Nota: È possibile disattivare l'accesso automatico a Windows facendo clic sul pulsante **Opzioni >>** nella finestra di dialogo di accesso e disattivando l'opzione **Accesso pass-through a Windows**. La disattivazione dell'accesso automatico è ad esempio necessaria per consentire ad altri utenti di utilizzare l'autenticazione all'accensione sullo stesso computer (*vedere Importazione di altri utenti* a pagina 7). Il responsabile della protezione definisce, nei relativi criteri, se attivare o meno l'opzione di accesso pass-through a Windows, e se è consentito modificare questa impostazione nella finestra di dialogo di accesso.

Ritardo di accesso nel caso di tentativo di accesso non riuscito

Se l'accesso all'autenticazione all'accensione non riesce, ad esempio in seguito ad un errore di digitazione della password, viene visualizzato un messaggio di errore ed entra in vigore un ritardo di accesso per il successivo tentativo. Il tempo di attesa viene incrementato ad ogni tentativo di accesso non riuscito. I tentativi non riusciti vengono registrati nel log.

Blocco del computer

A seconda delle impostazioni dei criteri, il computer può venire bloccato in seguito ad un determinato numero di tentativi di accesso non riusciti. Per sbloccare il computer, avviare una procedura di richiesta/risposta, *vedere Recupero mediante richiesta/risposta* a pagina 39.

4 Accesso a Windows Vista e Windows 7

Con i sistemi operativi Windows Vista e Windows 7, SafeGuard Enterprise offre un metodo di autenticazione aggiuntivo.

Se si disattiva l'opzione **Pass-through a Windows** nella finestra di dialogo di accesso dell'autenticazione all'accensione, viene visualizzata la finestra di dialogo di accesso a Windows Vista/Windows 7. In questa finestra di dialogo è possibile anche selezionare un metodo di autenticazione diverso.

Nota: L'utilizzo di un metodo di autenticazione diverso non significa che SafeGuard Enterprise non sia attivo sul computer. In questo caso l'accesso a SafeGuard Enterprise non viene effettuato durante l'accesso a Windows Vista, bensì dopo.

4.1 Accesso tramite SafeGuard Enterprise

Di solito l'accesso a Windows avviene automaticamente dopo aver immesso la password durante l'Autenticazione all'accensione. Se si disattiva l'opzione **Pass-through a Windows** nella finestra di dialogo dell'Autenticazione all'accensione e si utilizza il metodo SafeGuard Enterprise per accedere a Windows; SafeGuard Enterprise sarà disponibile con tutte le sue funzionalità dopo aver effettuato l'accesso a Windows Vista o Windows 7.

Le chiavi richieste sono disponibili e tutti i dati vengono cifrati e decifrati in base ai criteri definiti.

4.2 Accesso tramite il metodo di autenticazione di Windows Vista/Windows 7

Nella finestra di dialogo di accesso a Windows è possibile selezionare un metodo di autenticazione alternativo per accedere a Windows invece del metodo di autenticazione di SafeGuard Enterprise.

Se si utilizza il metodo di autenticazione di Windows Vista/Windows 7, l'accesso a SafeGuard Enterprise viene eseguito dopo l'accesso al sistema operativo.

Dopo aver effettuato l'accesso a Windows Vista/Windows 7, l'applicazione per l'autenticazione di SafeGuard Enterprise viene avviata automaticamente, se ciò risulta essere necessario al fine di sfruttare appieno le funzionalità di SafeGuard Enterprise.

A seconda delle impostazioni di accesso nell'amministrazione centralizzata, viene visualizzata o un finestra di dialogo per l'inserimento delle credenziali utente oppure una finestra per l'inserimento del PIN.

1. Immettere le credenziali o il PIN e cliccare su **OK**.

La funzionalità di SafeGuard Enterprise è ora disponibile e sarà possibile, ad esempio, accedere ai dati cifrati, se in possesso della chiave necessaria.

4.3 Sincronizzazione password in Windows Vista e Windows 7

SafeGuard Enterprise rileva automaticamente se la password di Windows è stata modificata e dunque non corrisponde più a quella memorizzata. Questa situazione si può verificare quando si modifica la password di Windows mediante una rete VPN, su un altro computer, o in Active Directory.

Se SafeGuard Enterprise rileva questo tipo di problema, l'utente ne riceve notifica, e viene richiesto l'inserimento della password precedente. Successivamente, la password memorizzata da SafeGuard Enterprise viene aggiornata con la nuova password di Windows.

La sincronizzazione della password avviene in due situazioni:

- Durante l'accesso
- Durante una procedura di blocco/sblocco di Windows.

5 Accesso mediante Lenovo Fingerprint Reader

Per accedere a computer, applicazioni e reti, gli utenti devono ricordare diversi password e PIN. Con un lettore di impronte digitali, è sufficiente passare un dito sul lettore per effettuare l'accesso senza bisogno di password o token.

È impossibile perdere o dimenticare le proprie credenziali. E non si corre il rischio che personale non autorizzato acceda a tali informazioni. L'utilizzo di lettori di impronte digitali semplifica quindi la procedura di accesso ed incrementa il livello di protezione.

SafeGuard Enterprise supporta l'accesso tramite impronte digitali per l'Autenticazione all'accensione così come per l'accesso a Windows. Ad esempio, è possibile accedere a un computer portatile Lenovo semplicemente passando un dito sul lettore integrato nel portatile stesso. La restante parte della procedura di accesso viene eseguita automaticamente. È, inoltre, possibile bloccare e sbloccare il desktop in Windows passando il dito sul lettore di impronte digitali.

I lettori di impronte digitali vengono direttamente integrati su certi computer portatili Lenovo. Per l'accesso mediante impronte digitali, è possibile anche utilizzare una tastiera USB esterna.

Nota:

- È possibile collegare un solo lettore di impronte digitali alla volta al computer.
- Le procedure di accesso mediante token o impronte digitali non possono essere combinate sullo stesso computer.
- L'accesso remoto mediante impronte digitali non è supportato.

5.1 Requisiti

Per utilizzare l'accesso mediante impronte digitali, è necessario soddisfare i requisiti descritti nelle sezioni seguenti:

Requisiti generali

- Hardware Lenovo.
- Lenovo Fingerprint Reader nel computer portatile o tastiera USB con lettore di impronte digitali.
- Il BIOS più recente (consigliabile).
- SafeGuard Enterprise
- Prima di SafeGuard Enterprise, è necessario installare la versione consigliata del software specifico del fornitore:
 - ThinkVantage Fingerprint per AuthenTecoppure
 - ThinkVantage Fingerprint per UPEK.
- Per criterio, il responsabile della protezione deve avere attivato l'accesso tramite impronte digitali.

Requisiti di sistema

- Windows XP, a 32 bit
- Windows Vista, a 32 bit, o a 64 bit
- Windows 7, a 32 bit, o a 64 bit

Hardware supportato

Per ulteriori informazioni sugli hardware supportati per l'accesso tramite impronte digitali, consultare l'articolo in inglese <http://www.sophos.com/support/knowledgebase/article/108789.html>.

Software supportato

Per ulteriori informazioni sui software supportati per le impronte digitali, consultare l'articolo in inglese <http://www.sophos.com/support/knowledgebase/article/111626.html>.

5.2 Registrazione delle impronte digitali

Per eseguire l'accesso al computer portatile/PC mediante impronte digitali, è innanzitutto necessario registrare una o più impronte utilizzando il software consigliato dal fornitore. La procedura di registrazione collega l'impronta registrata alle credenziali dell'utente (nome utente e password).

Prerequisiti: La procedura descritta di seguito prevede che siano installati sia il software consigliato dal fornitore sia SafeGuard Enterprise.

1. Eseguire l'accesso all'Autenticazione all'accensione (POA) inserendo nome utente e password.
2. Registrare una o più impronte digitali utilizzando il software installato dal fornitore. La procedura di registrazione collega l'impronta digitale alle credenziali di Windows.
 - a) Per informazioni su come registrare un'impronta digitale, consultare la relativa documentazione per il software ThinkVantage Fingerprint.
 - b) Abilitare l'opzione **POA password in BIOS** (solo UPEK, per AuthenTec questo passaggio non è necessario).
 - c) Per utilizzare l'accesso tramite impronte digitali nell'Autenticazione all'accensione, è necessario accedere a Windows una volta mediante le proprie impronte digitali, per trasferire le proprie credenziali all'apposito lettore. Per UPEK è sufficiente passare sul lettore l'impronta digitale registrata. Per AuthenTec è inoltre necessario immettere la password di Windows al primo accesso.
3. Riavviare il computer.
4. Per verificare l'impronta registrata, passare il dito sul lettore di impronte digitali dopo aver riavviato il computer.

Se l'impronta digitale corrisponde a quella registrata, l'accesso a Windows viene eseguito automaticamente.

5.3 Accesso all'Autenticazione all'accensione tramite impronta digitale

Prerequisiti:

- Il responsabile della protezione deve aver impostato l'opzione per le impronte digitali nel relativo criterio **Autenticazione**.

- È necessario registrare una o più impronte digitali.

1. Riavviare il computer.

Viene visualizzata la finestra di dialogo Autenticazione all'accensione per eseguire l'accesso tramite impronta digitale.

2. Passare una delle dita registrate sul lettore.

Se il software riconosce l'impronta digitale, l'Autenticazione all'accensione leggerà le credenziali e le invierà a Windows.

Nota: La procedura di accesso utilizza icone con brevi messaggi di testo come prompt, notifiche e avvisi (*vedere [Icane utilizzate durante la procedura di accesso](#) a pagina 24*).

L'accesso a Windows viene eseguito automaticamente, senza ulteriori richieste di dati.

Nota:



- Se la procedura di registrazione in Windows non viene completata correttamente (ad esempio, se dopo la registrazione delle impronte digitali non è stata eseguita la disconnessione e il nuovo accesso a Windows), nell'Autenticazione all'accensione sarà possibile reperire una corrispondenza con le impronte digitali registrate.








Tuttavia, non vi saranno credenziali. In questo caso, viene visualizzato un messaggio di errore in cui viene richiesto di accedere mediante nome utente e password, ma senza l'accesso pass-through a Windows. Le credenziali vengono trasferite al lettore di impronte digitali.


- Nei criteri applicabili all'utente il responsabile della protezione specifica se l'accesso pass-through a Windows è stato abilitato o disabilitato, e se è possibile modificare queste impostazioni nella finestra di dialogo Autenticazione all'accensione, per eseguire l'accesso mediante nome utente e password (*vedere [Accesso mediante nome utente e password](#) a pagina 26*).

5.3.1 Icone utilizzate durante la procedura di accesso

Quando si accede all'autenticazione all'accensione mediante impronte digitali, il sistema utilizza icone come prompt, notifiche e avvisi. Queste icone vengono visualizzate durante la procedura di accesso insieme a un breve messaggio di testo.

	<p>Richiede all'utente di passare il dito sul lettore di impronte digitali.</p>
	<p>Indica che l'accesso mediante impronte digitali non è attualmente abilitato. Questo può verificarsi se il modulo per l'accesso mediante impronte digitali non è ancora stato inizializzato.</p>

	<p>Indica che il lettore di impronte digitali è in funzione e occupato.</p>
	<p>Indica che l'impronta digitale è stata letta correttamente e che è stata trovata una corrispondenza.</p>
	<p>Indica che l'impronta digitale è stata letta correttamente, ma che non è stata trovata alcuna corrispondenza.</p>
	<p>Indica che non è stato possibile leggere l'impronta digitale. Passare nuovamente il dito sul lettore di impronte digitali.</p>
	<p>Indica che il dito è stato posizionato troppo a sinistra (o troppo a destra). Spostare il dito al centro del lettore di impronte digitali.</p>
	<p>Indica che il dito è stato passato troppo in obliquo. Passare nuovamente il dito sul lettore di impronte digitali.</p>
	<p>Indica che il dito è stato spostato troppo velocemente. Passare nuovamente il dito sul lettore di impronte digitali.</p>

	Indica che il dito è stato passato troppo velocemente. Passare nuovamente il dito sul lettore di impronte digitali.
---	---

5.3.2 Tentativi di accesso non riusciti

Se non è possibile leggere le impronte digitali dopo cinque tentativi, il tentativo di accesso viene ritenuto non riuscito e viene registrato come evento. In tal caso, entra in vigore un ritardo di accesso.

Se la lettura delle impronte digitali viene eseguita correttamente, ma dopo cinque tentativi non viene trovata alcuna corrispondenza con l'impronta registrata, anche questo viene considerato un tentativo di accesso non riuscito e registrato come evento. Anche in questo caso, entra in vigore un ritardo di accesso.

Il ritardo di accesso aumenta con ogni tentativo di accesso non riuscito.

5.3.3 Accesso mediante nome utente e password

Anche se l'accesso mediante impronte digitali è abilitato, è comunque possibile eseguire l'accesso all'Autenticazione all'accesso mediante nome utente e password, ad esempio, nel caso in cui non sia possibile accedere mediante impronte digitali a causa di un lettore difettoso.

1. Premere il tasto **Esc** oppure **Ctrl+Alt+Canc** nella finestra di dialogo Autenticazione all'accensione, per effettuare l'accesso mediante impronte digitali.

Viene visualizzata la finestra di dialogo Autenticazione all'accensione per eseguire l'accesso tramite nome utente e password.

Nota: Se si preme **Ctrl+Alt+Canc** nella finestra di dialogo Autenticazione all'accensione per l'accesso tramite nome utente e password, il computer viene arrestato. In questa finestra, **Ctrl+Alt+Canc** equivale al pulsante **Arresta il sistema**.

La finestra di dialogo dell'autenticazione all'accensione per l'accesso mediante nome utente e password viene visualizzata automaticamente se il lettore delle impronte digitali non è disponibile o se non vengono trovati dati utente nel lettore.

Nota: L'accesso mediante nome utente e password viene abilitato automaticamente se la cache locale è danneggiata. In tal caso, il computer verrà bloccato e sarà necessario effettuare l'accesso utilizzando la procedura Challenge/Response.

2. In alternativa, premere nuovamente **Esc** per tornare alla finestra di dialogo Autenticazione all'accensione per accedere con impronte digitali.

Se è stato premuto **Esc** per passare alla finestra di dialogo dell'autenticazione all'accensione per accedere mediante nome utente e password, è ancora possibile eseguire l'accesso passando il dito sul lettore senza dover prima tornare alla finestra di dialogo dell'autenticazione all'accensione per accedere tramite impronte digitali.

5.4 Modifica della password

1. Se l'accesso mediante impronte digitali è abilitato nell'Autenticazione all'accensione, è possibile modificare la password in Windows premendo **Ctrl+Alt+Canc**.

Dopo aver modificato la password, viene richiesto di passare il dito sul lettore di impronte digitali in modo da trasferire la nuova password al lettore.

Nota:

Se la password viene modificata, la modifica viene applicata a tutte le impronte digitali registrate.

5.4.1 Sincronizzazione della password

Se la password di Windows non corrisponde più alla password memorizzata nel lettore di impronte digitali, ad esempio, nei casi in cui la password è stata modificata ma la nuova password non è stata trasferita al lettore di impronte digitali, è possibile sincronizzare la password.

1. Riavviare il computer.
2. Premere il tasto **Esc** oppure **Ctrl+Alt+Canc** nella finestra di dialogo dell'Autenticazione all'accensione, per effettuare l'accesso mediante impronte digitali. Questa operazione riporta alla finestra di dialogo dell'Autenticazione all'accensione per l'accesso tramite nome utente e password.
3. Fare clic su **Opzioni**, e disabilitare l'opzione **Accesso pass-through a Windows**.

Nota: Nei criteri applicabili all'utente il responsabile della protezione specifica se l'accesso pass-through a Windows è stato abilitato o disabilitato, e se è consentito modificare queste impostazioni nella finestra di dialogo dell'autenticazione all'accensione per eseguire l'accesso mediante nome utente e password.

4. Accedere con la propria password.
5. Viene visualizzata la finestra di dialogo di accesso a Windows. Passare una delle dita registrate sul lettore di impronte digitali.
6. L'impronta viene riconosciuta dal sistema, ma Windows rifiuta la password collegata all'impronta digitale. Questa situazione non viene identificata come un tentativo di accesso non riuscito e, di conseguenza, non viene effettuato un accesso posticipato.

Viene visualizzato un messaggio che indica che la password è stata modificata e viene richiesto di inserire la password di Windows corrente.

7. Inserire la password di Windows corretta.

Nota:

Se si inserisce una password di Windows errata, viene registrato un tentativo di accesso non riuscito, ed entra in vigore un ritardo di accesso. Allo stesso modo, se viene chiusa la richiesta di input senza inserire la password, viene registrato un tentativo di accesso non riuscito e viene effettuato un accesso posticipato.

Il corretto trasferimento della password completa il suo processo di sincronizzazione; la password potrà quindi essere utilizzata per l'accesso.

5.5 Recupero dell'accesso tramite impronte digitali

Se l'accesso tramite impronte digitali non funziona e non si ricorda la password necessaria per effettuare l'accesso, SafeGuard Enterprise mette a disposizione i seguenti metodi di recupero:

- Recupero tramite Local Self Help, [vedere Recupero tramite Local Self Help](#) a pagina 29.
- Recupero tramite Challenge/Response, [vedere Recupero mediante richiesta/risposta](#) a pagina 39.

I metodi di recupero disponibili per il proprio computer dipendono dalle impostazioni scelte dal responsabile della protezione.

Per dare inizio al recupero, cliccare sul pulsante **Recupero** nella finestra di dialogo relativa all'accesso mediante impronte digitali.

Nota:

In seguito alla procedura di recupero, potrebbe venire richiesta la modifica della password al avvio del computer, per abilitare, ad esempio, il recupero in caso di password dimenticata. In questo caso, il sistema consente di aggiornare le credenziali delle impronte digitali.

6 Opzioni di recupero

SafeGuard Enterprise offre varie opzioni di recupero (ad esempio, nel caso si sia dimenticata la password), personalizzate a seconda dei diversi scenari di recupero:

- **Recupero dell'accesso con Local Self Help**

Nel caso si sia dimenticata la password, l'utente può accedere al computer mediante Local Self Help senza richiedere assistenza all'help desk. Anche in situazioni in cui non sono disponibili connessioni telefoniche o di rete (ad esempio a bordo di un aeromobile), è possibile recuperare l'accesso al proprio computer. A tale scopo, è sufficiente rispondere a una serie di domande predefinite nell'autenticazione all'accensione.

Per ulteriori informazioni, [vedere Recupero tramite Local Self Help](#) a pagina 29.

- **Recupero mediante richiesta/risposta**

Il meccanismo richiesta/risposta è un sistema di recupero sicuro ed efficace, che risulta molto utile nel caso in cui non si sia in grado di accedere ai propri computer o dati cifrati. Durante la procedura di richiesta/risposta, l'utente fornisce un codice di richiesta generato

dal computer all'addetto all'helpdesk, il quale a sua volta genera un codice di risposta che autorizza l'utente a eseguire una determinata azione sul proprio computer.

Per ulteriori informazioni, [vedere Recupero mediante richiesta/risposta](#) a pagina 39.

Entrambe le opzioni di recupero vengono attivate dal responsabile della protezione nei criteri, per l'utilizzo sul computer dell'utente.

7 Recupero tramite Local Self Help

Se la password è stata dimentica e non è possibile contattare l'helpdesk per ricevere assistenza, SafeGuard Enterprise offre Local Self Help.

Local Self Help permette di recuperare l'accesso al proprio notebook anche in mancanza di connessione telefonica o ad una rete, o, ancora, in caso non sia possibile eseguire la procedura Challenge/Response (ad esempio, a bordo di un aereo). È possibile accedere al computer rispondendo ad un determinato numero di domande predefinite nell'autenticazione all'accensione.

Il responsabile della protezione può stabilire le domande a cui rispondere e distribuirle ai computer endpoint. In alternativa, l'utente può creare le proprie domande, laddove il criterio applicato lo autorizzi a farlo. La procedura guidata di Local Self Help assiste durante l'inserimento delle risposte iniziali e la modifica delle domande. Per aprire la procedura guidata di Local Self Help, fare clic sull'icona di SafeGuard Enterprise, situata nell'area di notifica sulla barra delle applicazioni di Windows.

Il recupero tramite Local Self Help, nell'Autenticazione all'accensione, è a disposizione per i seguenti metodi di accesso.

- Accesso tramite ID utente e password
- Accesso tramite impronta digitale
- Accesso tramite token non di cifratura, fermo restando che l'accesso tramite ID utente e password sia stato abilitato dal criterio come possibile modalità di accesso.

Prerequisiti

Per utilizzare Local Self Help per il recupero dell'accesso, è necessario che i seguenti prerequisiti vengano soddisfatti:

- Il responsabile della protezione deve aver abilitato Local Self Help nel relativo criterio e definito le impostazioni per questa funzione (ad esempio, l'autorizzazione a creare domande).
- Local Self Help deve essere attivato sul computer dell'utente ([vedere Attivazione di Local Self Help](#) a pagina 29).

7.1 Attivazione di Local Self Help

Una volta divenuto effettivo il criterio che autorizza l'utente all'utilizzo di Local Self Help, sarà necessario attivare la funzione rispondendo alle domande predefinite ricevute oppure rispondendo alle domande definite dall'utente stesso.

Local Self Help viene attivato sul computer dell'utente solo dopo che questo abbia risposto e salvato un numero predefinito di domande. Il responsabile della protezione indica a quante

domande l'utente dovrà rispondere. La procedura guidata di Local Self Help accompagna attraverso questo processo e mostra quante risposte sono richieste. A seconda delle impostazioni dei criteri, si possono verificare le seguenti situazioni:

■ **L'utente ha ricevuto le domande predefinite e non è autorizzato a determinarne di nuove.**

Rispondere e salvare le domande predefinite ricevute. La procedura guidata di Local Self Help mostra quante risposte sono richieste.

■ **L'utente ha ricevuto le domande predefinite ed è autorizzato a creare le domande personalmente.**

Rispondere e salvare il numero di domande richiesto (le domande predefinite, le domande impostate personalmente oppure una combinazione fra i due tipi).

■ **L'utente non ha ricevuto le domande predefinite ma è autorizzato a creare le domande personalmente.**

Creare, rispondere e salvare il numero di domande richiesto.

Nota: Per accedere all'Autenticazione all'accensione tramite Local Self Help, è necessario rispondere a domande selezionate casualmente fra le domande a cui si è risposto durante l'esecuzione della procedura guidata di Local Self Help. Il responsabile alla protezione indica a quante domande rispondere in POA.

Prerequisito: Una volta ricevuto il criterio, una notifica informa l'utente che sono presenti delle domande di Local Self Help cui non è stato risposto. Riavviare il computer per aggiungere il comando **Local Self Help** al menu di scelta rapida dell'icona dell'area di notifica nella barra delle applicazioni di Windows.

Per attivare Local Self Help:

1. Cliccare con il tasto destro del mouse sull'icona di Sophos SafeGuard nell'area di notifica, nella barra delle applicazioni di Windows.
2. Selezionare **Local Self Help**.

Viene visualizzata la finestra di dialogo di **benvenuto** della procedura guidata di Local Self Help.

Per motivi di sicurezza verrà richiesto di inserire la password.

3. Inserire la password e fare clic su **Avanti**.

Viene visualizzata la finestra di dialogo **Panoramica sullo stato**.

Questa finestra di dialogo spiega come attivare Local Self Help. Visualizza inoltre informazioni relative allo stato (ad esempio, il numero di domande impostate dall'utente a cui è stata data una risposta, il numero di domande predefinite con una risposta, ecc.).

4. Cliccare su **Avanti**.

Se si ricevono le domande predefinite assieme al criterio in vigore, viene visualizzata la finestra di dialogo **Predefined questions**.

- Se l'utente ha ricevuto domande relative a vari argomenti, può selezionare quale di questi visualizzare nell'elenco a discesa del campo **Tema**.
- Per visualizzare tutti gli argomenti in un elenco completo, selezionare l'opzione (predefinita) **Tutti i temi** dall'elenco a discesa.
- Per rispondere alle domande, cliccare sulla domanda e inserire la risposta nella colonna **Risposte**.
- Una volta inserita la risposta, il testo inserito viene nascosto. Per visualizzare il testo, selezionare **Mostra risposte**.

Nota: Quando si risponde alle domande durante un processo di recupero nell'autenticazione all'accensione, è necessario immettere le risposte esattamente nello stesso modo in cui sono state inserite durante la procedura guidata Local Self Help. In Local Self Help, per le risposte viene fatta distinzione fra maiuscole e minuscole.

Nota:

Quando si inseriscono risposte in giapponese, è necessario utilizzare i caratteri romaji (romani). Altrimenti, non vi sarà una corrispondenza fra le risposte al momento del loro inserimento nell'autenticazione all'accensione.

5. Una volta risposto alle domande predefinite, cliccare su **Avanti**.

6. Se in possesso del diritto di impostare le proprie domande, verrà visualizzata la finestra di dialogo **Domande definite dall'utente e risposte**.

- a) Per aggiungere una nuova domanda, cliccare su **Nuova domanda**.

All'elenco delle domande viene aggiunta una riga.

- b) Inserire la domanda nella colonna **Domande** e la relativa risposta nella colonna **Risposte**.

Una volta immessa la risposta, il testo inserito viene nascosto.

- c) Per visualizzare il testo, selezionare **Mostra risposte**.

Nota:

Quando si risponde alle domande durante un processo di recupero nell'autenticazione all'accensione, è necessario immettere le risposte esattamente nello stesso modo in cui sono state inserite durante la procedura guidata Local Self Help. In Local Self Help, per le risposte viene fatta distinzione fra maiuscole e minuscole.

Nota:

Quando si inseriscono risposte in giapponese, è necessario utilizzare i caratteri romaji (romani). Altrimenti, non vi sarà una corrispondenza fra le risposte al momento del loro inserimento nell'autenticazione all'accensione.

7. Una volta risposto alle domande definite personalmente, cliccare su **Avanti**.

Dopo aver risposto alle domande, l'ultima finestra di dialogo della procedura guidata di Local Self Help fornisce informazioni sul nuovo stato. Un messaggio indica se i prerequisiti per l'attivazione di Local Self Help siano stati soddisfatti o meno.

8. Cliccare su **Fine**.

Le domande e le risposte vengono salvate. Viene visualizzato un messaggio che indica che l'attivazione di Local Self Help è riuscita.

9. Cliccare su **OK**.

Local Self Help è attivo sul computer in uso. È possibile utilizzare Local Self Help per il recupero dell'accesso nell'autenticazione all'accensione.

Nota:

Se Local Self Help è attivo sul computer ed è stata reimpostare la password mediante una procedura di Challenge/Response, le risposte memorizzate in Local Self Help non sono più valide. Local Self Help non è più attivo sul computer. Per riattivare Local Self Help, rispondere nuovamente alle domande.

7.2 Modifica delle domande

Dopo l'attivazione di Local Self Help sul computer, è possibile modificare le domande in qualsiasi momento:

- Per le domande predefinite è possibile modificare le risposte fornite la prima volta che si procede all'inserimento delle risposte. Tuttavia, le domande predefinite non possono essere eliminate.
- Per le domande definite dall'utente, è possibile modificare le risposte fornite la prima volta che si procede all'inserimento delle risposte, aggiungere ed eliminare domande.

1. Cliccare con il tasto destro del mouse sull'icona di Sophos SafeGuard nell'area di notifica, nella barra delle applicazioni di Windows.
2. Selezionare **Local Self Help**.

Viene visualizzata la finestra di dialogo di **benvenuto** della procedura guidata di Local Self Help.

Per motivi di sicurezza verrà richiesto di inserire la password.

3. Inserire la password e fare clic su **Avanti**.

Viene visualizzata la finestra di dialogo **Panoramica sullo stato**.

Questa finestra di dialogo spiega come attivare Local Self Help. Visualizza inoltre informazioni relative allo stato (ad esempio, il numero di domande impostate dall'utente a cui è stata data una risposta, il numero di domande predefinite con una risposta, ecc.).

4. Cliccare su **Avanti**.

- a) Nel caso in cui l'utente abbia ricevuto e risposto alle domande predefinite, viene visualizzata la finestra di dialogo **Domande predefinite**, in cui vengono indicate le risposte.
- b) Se l'utente ha ricevuto domande relative a vari argomenti, può selezionare quale di questi visualizzare nell'elenco a discesa del campo **Tema**.
- c) Per visualizzare tutti gli argomenti in un elenco completo, selezionare l'opzione (predefinita) **Tutti i temi** dall'elenco a discesa.

Per impostazione predefinita, le risposte inserite non vengono visualizzate come testo.

- d) Per visualizzare il testo inserito, selezionare la casella di spunta **Mostra risposte**.
- e) Per modificare le risposte, cliccare sulle relative domande e inserire la nuova risposta nella colonna **Risposte**.

5. Per completare l'operazione di modifica, cliccare su **Avanti**.

Se in possesso del diritto di impostare le proprie domande, verrà visualizzata la finestra di dialogo **Domande definite dall'utente e risposte**. Per impostazione predefinita, le risposte inserite non vengono visualizzate come testo.

6. Per visualizzare il testo inserito, cliccare sulla casella di spunta **Mostra risposte**.

- a) Per modificare le risposte esistenti, cliccare sulle relative domande e inserire la nuova risposta nella colonna **Risposte**.
- b) Per aggiungere una nuova domanda, cliccare su **Nuova domanda**.

All'elenco delle domande viene aggiunta una riga. Inserire la domanda nella colonna **Domande** e la relativa risposta nella colonna **Risposte**.

- c) Per eliminare alcune domande, cliccare sulla domanda desiderata e selezionare il pulsante **Elimina domanda**.

Viene visualizzato un messaggio che richiede conferma di voler eliminare la domanda. Cliccare su **Sì**.

7. Completata l'operazione di modifica, cliccare su **Avanti**.

Dopo aver modificato le domande, l'ultima finestra di dialogo della procedura guidata di Local Self Help fornisce informazioni sul nuovo stato. Un messaggio indica se i prerequisiti necessari perché Local Self Help rimanga attivo siano stati soddisfatti o meno.

8. Cliccare su **Fine**.

Le domande e le risposte vengono salvate. Viene visualizzato un messaggio che indica che la procedura di modifica è riuscita e che Local Self Help resterà attivo.

9. Cliccare su **OK**.

Le modifiche apportate divengono attive.

Al successivo avvio di Local Self Help nell'autenticazione all'accensione verranno selezionate e visualizzate casualmente le domande modificate/nuove, alle quali saranno applicate le risposte modificate/nuove.

Nota:

Qualora il numero di domande con risposta divenisse inferiore al numero minimo richiesto a causa delle modifiche apportate, viene visualizzato un messaggio di errore nell'ultima finestra di dialogo che informa l'utente che al termine della procedura guidata Local Self Help verrà disattivato. Se non si desidera disattivarlo, è possibile tornare alla finestra di dialogo **Domande definite dall'utente** e **Domande predefinite**, facendo clic sul pulsante **Indietro**. Sarà quindi possibile aggiungere o rispondere a nuove domande. Se si seleziona **Fine** e il numero di domande con risposta è inferiore a quello minimo richiesto, viene visualizzato un ulteriore messaggio di avviso, che informa che Local Self Help non sarà più attivo sul computer dell'utente. In questo caso è comunque possibile riattivare Local Self Help (*vedere Attivazione di Local Self Help* a pagina 29).

7.3 Parametri di modifica delle domande

Il responsabile alla protezione può definire i seguenti parametri da applicare alle domande di Local Self Help:

- Il numero di domande a cui rispondere nella procedura guidata di Local Self Help, per attivarlo nel proprio computer. Si deve stabilire il numero di domande specificato e le relative risposte per poter mantenere attivo il Local Self Help.
- Il numero di domande a cui rispondere in POA per poter accedere a Local Self Help. Le domande visualizzate in POA vengono scelte in modo casuale fra quelle a cui si è dato risposta durante la procedura guidata di Local Self Help.

Se questi due parametri vengono modificati a cause dell'introduzione di un nuovo criterio distribuito al computer, si potrebbero verificare le seguenti situazioni:

Condizione	Azione di LSH	Richiesta azione dell'utente
Il numero di domande a cui rispondere nella procedura guidata di LSH Wizard viene modificato, ma il numero di domande a disposizione di Local Self Help è sufficiente per mantenerlo attivo nel computer.	Local Self Help resta attivo nel computer.	Nessuna.
Il numero di domande a cui rispondere nella procedura guidata di LSH viene modificato, ma il numero di domande a disposizione di Local Self Help non è sufficiente per mantenerlo attivo nel computer.	Viene visualizzato un messaggio in cui si informa che le impostazioni di Local Self Help sono state modificate. Le domande a disposizione nel proprio computer non sono più valide. Local Self Help non è più attivo sul computer.	Per riattivare Local Self Help, aprire la procedura guidata di Local Self Help, e seguire le istruzioni.

Condizione	Azione di LSH	Richiesta azione dell'utente
Il numero di domande a cui rispondere in POA per accedere a Local Self Help viene modificato.	Viene visualizzato un messaggio in cui si informa che le impostazioni di Local Self Help sono state modificate. Le domande a disposizione nel proprio computer restano non valide. La proporzione fra numero di domande disponibili e risposte valide è cambiata.	Aprire la procedura guidata di Local Self Help e seguirne le istruzioni.

7.4 Cambiamento di condizioni o parametri di Local Self Help durante processi di modifica

I parametri di Local Self Help e altre condizioni essenziali per l'utilizzo di Local Self Help possono cambiare mentre l'utente definisce o modifica domande all'interno della procedura guidata di Local Self Help.

Per esempio:

- Viene creata una nuova password o un nuovo certificato utente.
- Nuovi criteri con nuove impostazioni di Local Self Help e/o una nuova serie di domande di Local Self Help possono venire trasferiti sul computer dell'utente tramite meccanismi di aggiornamento ordinari.

Se si verificano tali cambiamenti durante il processo di modifica, la serie di domande e risposte appena definita potrebbe non essere più valida; potrebbe quindi non essere presente un numero sufficiente di domande di Local Self Help, per consentire a quest'ultimo di rimanere attivo nel computer dell'utente.

Di conseguenza, ogni qualvolta si termini di definire o modificare domande nella procedura guidata Local Self Help, essa controlla se siano applicabili le seguenti condizioni, ed intraprende la relativa azione:

Condizione	Azione della procedura guidata di LSH	Risultato
Un nuovo criterio ha disabilitato Local Self Help a livello globale.	La procedura guidata Local Self Help visualizza un messaggio che segnala la disabilitazione di Local Self Help a livello globale, e chiude la finestra.	Non è più possibile utilizzare Local Self Help.
Un nuovo criterio ha modificato i parametri di Local Self Help (ad esempio, la lunghezza minima dei caratteri all'interno delle risposte, l'autorizzazione a creare domande, o il numero di domande a cui rispondere sono parametri revocati). Tuttavia,	La procedura guidata Local Self Help visualizza un messaggio che segnala la modifica dei parametri di Local Self Help, e chiude la finestra.	Local Self Help è attivo sul computer in uso, e può essere utilizzato per recuperare l'accesso. Tuttavia, la proporzione fra numero di domande disponibili e risposte valide potrebbe essere

Condizione	Azione della procedura guidata di LSH	Risultato
<p>Local Self Help non è stato disabilitato.</p> <p>Le domande e le risposte definite dall'utente sono ancora valide e sono sufficienti a mantenere Local Self Help attivo sul computer.</p>		<p>cambiata. Per riportarla alle condizioni originarie, potrebbe essere necessario aggiungere o eliminare domande o risposte.</p>
<ul style="list-style-type: none"> ■ La password utente è stata modificata e/o ■ Un nuovo criterio ha modificato i parametri di Local Self Help (ad esempio, la lunghezza minima dei caratteri all'interno delle risposte, o l'autorizzazione a creare domande, o il numero di domande a cui rispondere). Local Self Help non è stato disabilitato. <p>Tuttavia, le domande e le risposte definite dall'utente non sono più valide e non è presente una numero sufficiente di domande per mantenere Local Self Help attivo sul computer.</p>	<p>La procedura guidata Local Self Help visualizza un messaggio che segnala che la password utente o i parametri di Local Self Help sono stati modificati. Local Self Help non è più attivo sul computer dell'utente. All'utente viene consigliato di eseguire nuovamente la procedura guidata. La procedura guidata viene terminata.</p>	<p>Per attivare Local Self Help, eseguire di nuovo la procedura guidata Local Self Help, e definire nuovamente domande e risposte. Successivamente, sarà possibile utilizzare Local Self Help per il recupero dell'accesso.</p>
<p>Il certificato utente è stato modificato.</p>	<p>La procedura guidata Local Self Help visualizza un messaggio che segnala che il certificato utente è stato modificato. Local Self Help non è più attivo sul computer dell'utente. All'utente viene consigliato di eseguire nuovamente la procedura guidata. La procedura guidata viene terminata.</p>	<p>Per attivare Local Self Help, eseguire di nuovo la procedura guidata Local Self Help, e definire nuovamente domande e risposte. Successivamente, sarà possibile utilizzare Local Self Help per il recupero dell'accesso.</p>

7.5 Accesso all'Autenticazione all'accensione mediante Local Self Help

1. Nella finestra di dialogo dell'Autenticazione all'accensione, cliccare sul pulsante **Recupero**.
 - Se per il recupero dell'accesso è attivo solo Local Self Help, questo si avvia.
 - Se Challenge/Response e Local Self Help sono disponibili per il recupero dell'accesso, viene visualizzata una finestra di dialogo per la selezione, indicante entrambe le modalità di recupero. Cliccare su **Local Self Help**.

Nota:

Se si è soliti accedere all'Autenticazione all'accensione tramite PIN o smartcard, è per prima cosa necessario rimuovere il PIN o la smartcard dal computer. Viene quindi visualizzata la finestra di dialogo per eseguire l'accesso mediante nome utente e password. Inserire l'ID dell'utente e cliccare sul pulsante **Recupero**.

Viene visualizzata la finestra di dialogo **Benvenuti a Local Self Help**.

Questa finestra fornisce una breve descrizione dei passaggi che seguiranno.

2. Cliccare su **Avanti** per iniziare a rispondere alle domande.

La prima domanda viene visualizzata.
3. Inserire la risposta.

Per impostazione predefinita, il testo inserito non viene visualizzato nel campo di inserimento per motivi di sicurezza. Per visualizzare la risposta, deselezionare la casella di controllo **Nascondi risposta**.
4. Dopo aver risposto alla domanda, cliccare su **Avanti**.

Una volta risposto a una domanda, cliccare su **Avanti** e procedere con quella successiva.
5. Rispondere alle restanti domande. Dopo aver risposto all'ultima, cliccare su **OK**.

Nella finestra di dialogo successiva è possibile visualizzare la password corrente.
6. Per visualizzare la password, premere **Invio** o la **barra spaziatrice**, oppure cliccare sulla finestra blu.

Nota:

NON cliccare su **OK**. Dopo aver cliccato su **OK** il processo di avvio continuerà infatti **SENZA** che la password venga visualizzata.

La password verrà mostrata per un intervallo di tempo massimo di 5 secondi. In seguito, il processo di avvio continuerà automaticamente.

Nota:

Assicurarsi che nessun utente non autorizzato possa vedere, involontariamente o volontariamente, il contenuto della schermata. È possibile nascondere immediatamente la propria password, premendo la **barra spaziatrice**, **Invio**, oppure cliccando sulla finestra blu.

7. È possibile leggere la password e utilizzarla per l'accesso durante l'autenticazione all'accensione e successivamente per accedere nuovamente a Windows.
8. Dopo aver letto la password, fare clic su **OK**. In caso contrario, il processo di avvio continuerà automaticamente dopo 5 secondi dalla visualizzazione della password.

Si dispone ora dell'accesso all'autenticazione all'accensione e a Windows.

7.6 Tentativi di accesso non riusciti

Se per una o più domande si inserisce una risposta errata, non sarà possibile accedere. In tal caso verrà visualizzato un messaggio che indica che l'accesso non è riuscito. Per ragioni di sicurezza, Local Self Help non indica la risposta incorretta fra quelle inserite.

Una procedura di recupero di Local Self Help non riuscita viene considerata come un tentativo di accesso non riuscito, e registrata come evento. In tal caso, entra in vigore un ritardo di accesso. Il ritardo di accesso aumenta con ogni tentativo di accesso non riuscito.

Se il computer viene riavviato in seguito a un tentativo di accesso non riuscito, e si opta nuovamente per il recupero dell'accesso mediante Local Self Help, saranno nuovamente selezionate domande a caso.

7.7 Riattivazione di domande e risposte dopo aver modificato la password di diversi computer

Se Local Self Help è attivato su diversi computer e viene modificata la password di Windows su uno di tali computer, una volta che tale modifica sia divenuta effettiva, le domande e le risposte memorizzate in Local Self Help non saranno più valide sui restanti computer. Tuttavia, le domande e le risposte saranno ancora disponibili nella procedura guidata Local Self Help. Per utilizzare nuovamente lo stesso insieme di domande sul secondo computer, confermarle mediante la procedura guidata Local Self Help.

1. Una volta modificata la password sul computer in questione, accedere al secondo computer.
Una notifica informa l'utente che sono presenti delle domande di Local Self Help cui non è stato risposto.
2. Cliccare col tasto destro del mouse sull'icona SafeGuard Enterprise System dell'area di notifica nella barra delle applicazioni di Windows e selezionare **Local Self Help**.
Viene visualizzata la finestra di dialogo di **benvenuto** della procedura guidata di Local Self Help.
3. Inserire la password e cliccare su **Avanti**.
4. Confermare tutte le pagine della procedura guidata Local Self Help, selezionando **Avanti** e cliccando su **Fine** nell'ultima pagina.

Le domande e le risposte memorizzate in precedenza nel computer tornano di nuovo attive e vengono utilizzate per l'accesso mediante l'Autenticazione all'accensione via Local Self Help.

8 Recupero mediante richiesta/risposta

Come recupero, SafeGuard Enterprise offre una **procedura Challenge/Response** che consente lo scambio di informazioni riservate.

Se si utilizza SafeGuard Enterprise e, ad esempio, si è dimenticata la password, è possibile recuperare l'accesso al computer rapidamente con l'aiuto di un help desk centrale.

Nota:

Si consiglia di utilizzare il Local Self Help per il recupero di una password dimenticata. Local Self Help permette di visualizzare la password corrente e di continuare ad utilizzarla. Ciò evita il bisogno di reimpostarla, o di coinvolgere l'helpdesk.

Durante la procedura di richiesta/risposta, l'utente genera un codice di richiesta (una stringa di caratteri ASCII) e fornisce tale codice a un membro del personale dell'helpdesk. In base al codice di richiesta fornito, l'addetto all'helpdesk genera a sua volta un codice di risposta che autorizza l'utente a eseguire una determinata azione sul proprio computer.

Il recupero tramite Challenge/Response, nell'Autenticazione all'accensione, è disponibile solo per i seguenti metodi di accesso:

- Tramite ID e password.
- Tramite impronta digitale.
- Tramite token non di cifratura.

8.1 Scenari tipo in cui potrebbe essere necessario richiedere assistenza all'help desk

- L'utente ha dimenticato la password.
- È stata immessa troppe volte una password incorretta. Il computer è stato bloccato.
- L'utente ha dimenticato o ha perso il token/la smartcard.
- La cache locale di Autenticazione all'accensione è parzialmente danneggiata.
- Il computer protetto da SafeGuard Enterprise deve essere avviato da un altro utente.
- Un utente deve avviare il computer protetto da SafeGuard Enterprise mediante un supporto esterno.

8.2 Procedure per le quali è possibile richiedere un codice response e i relativi scenari

■ Avvio del clientSafeGuard Enterprise senza l'accesso utente

L'avvio del computer senza l'accesso utente è utile se è stata inserita una password non corretta (ad esempio contenente errori di digitazione, attivando il tasto BLOC MAIUSC e così via), ma l'utente è a conoscenza della password corretta. La procedura Challenge/Response consente di accedere al computer senza reimpostare la password.

Se una password incorretta è stata immessa troppe volte, l'help desk genera automaticamente un codice response per consentire l'avvio del client senza l'accesso utente. Il requisito per questo caso specifico è contenuto nella challenge. Successivamente sarà possibile accedere nuovamente con il nome utente e la password.

■ **Avvio del client SafeGuard Enterprise con l'accesso utente**

Se si è dimenticata la password, non tentare di immetterne una, ma richiedere una challenge. L'help desk potrà quindi generare un codice response per l'accesso con o senza un nome utente. Quando si accede utilizzando il proprio nome utente, chiedere all'help desk di visualizzare la propria password durante una procedura Challenge/Response. Ciò evita di dover reimpostare la password. In alternativa, quando si effettua l'accesso con il nome utente, è necessario reimpostare la propria password per l'accesso a Windows durante la procedura Challenge/Response.

Nota: Per gli utenti che lavorano in modalità non in linea, ovvero senza essere connessi al controller di dominio, è necessario tenere in considerazione alcuni aspetti particolari ([vedere Challenge/Response per utenti non in linea](#) a pagina 44).

■ **Ripristino della cache dei criteri di SafeGuard Enterprise:**

Questa procedura è necessaria se la cache dei criteri è danneggiata. La cache locale memorizza tutte le chiavi, i criteri, i certificati utente e i file audit. Per impostazione predefinita, se la cache locale è danneggiata il recupero dell'accesso viene disattivato, ovvero, verrà ripristinato automaticamente mediante backup. In tal caso, per riparare la cache locale non è richiesta la procedura Challenge/Response. Tuttavia, se la cache viene riparata in modo esplicito mediante una procedura di richiesta/risposta, è possibile attivare il recupero dell'accesso mediante criteri. In questo caso, se la cache locale è danneggiata, viene richiesto automaticamente di avviare una procedura di richiesta/risposta.

■ **Avvio da un supporto esterno o da disco floppy:**

La procedura Challenge/Response può essere utilizzata anche per consentire l'avvio di un computer da un supporto esterno. Per far ciò, selezionare **Disco floppy/supporto esterno** nel campo **Continua l'avvio da** della finestra di dialogo dell'Autenticazione all'accensione e iniziare la procedura Challenge/Response. L'help desk potrà quindi generare un codice response per le seguenti azioni:

- Avvio del client SGN con l'accesso utente
- Avvio del client SGN senza l'accesso utente
- Consentire la procedura di avvio da supporti esterni

8.3 Procedura Challenge/Response

1. Viene avviata l'Autenticazione all'accensione.

Nota: Durante una procedura di Challenge/Response, quando viene generata la challenge, si ha a disposizione un intervallo di tempo di 30 minuti, entro il quale va inserita la response generata dall'help desk. Allo scadere dei 30 minuti, il codice di risposta non sarà più valido e non potrà più essere utilizzato.

2. Richiesta di una challenge:

Aprire la finestra di dialogo **Challenge** nell'Autenticazione all'accensione. Viene generato e visualizzato un codice challenge sotto forma di stringa di caratteri ASCII.

3. Contattare l'help desk.

Insieme al codice challenge, comunicare i propri dati utente (ID utente, ID computer, ecc.) come descritto nella finestra di dialogo **Challenge**

4. L'help desk genera un codice response tramite il SafeGuard Management Center.

5. L'help desk fornisce all'utente il codice response tramite telefono o SMS.

6. Inserire il codice response al momento dell'Autenticazione all'accensione.

L'utente ora può eseguire l'azione per la quale è stato autorizzato. Ad esempio, può reimpostare la password.

A questo punto è possibile riprendere il lavoro.

8.4 Richiesta di una challenge:

1. Nella finestra di dialogo di accesso dell'Autenticazione all'accensione cliccare su **Recupero**.

Il pulsante **Recupero** viene attivato soltanto quando si inserisce un nome utente o almeno un carattere nella finestra di dialogo del PIN.

Nota: Se è stata inserita troppe volte una password o PIN non corretti o se la cache dei criteri è danneggiata, SafeGuard Enterprise informa automaticamente l'utente, al quale viene proposto di risolvere il problema tramite Challenge/Response.

Vengono visualizzati i dati dell'utente e un codice challenge generato casualmente. Per facilitarne la lettura, il codice challenge è diviso in blocchi di 5 caratteri ciascuno.

2. Chiamare l'help desk di SafeGuard Enterprise e fornire al responsabile i propri dati utente insieme al codice challenge.

Se si riscontrassero difficoltà nel digitare il codice challenge, cliccare sul pulsante **Correzione ortografica**.

Il responsabile dell'help desk può identificare lo scenario adeguato dal codice challenge.

3. Cliccare su **Avanti**.

8.5 Inserimento del codice response

1. Inserire il codice response ricevuto dal responsabile dell'help desk nella finestra di dialogo **Response** e cliccare su **OK**.

Se si inserisce il codice response in modo non corretto, il blocco di caratteri contenente l'errore viene contrassegnato con il colore rosso.

2. L'utente è ora connesso all'autenticazione all'accensione.

Se necessario, SafeGuard Enterprise richiederà di modificare le proprie credenziali utente di Windows.

8.6 Procedura consigliata

8.6.1 È stata immessa troppe volte una password non valida

È stata immessa troppe volte una password non valida nell'Autenticazione all'accensione (errori di battitura, attivazione del tasto Bloc Maiusc, ecc.), ma si conosce quella giusta. L'utente è connesso al dominio.

1. Il computer è bloccato. Viene chiesto di iniziare una procedura Challenge/Response per sbloccare il computer.
2. Il responsabile dell'help desk genera un codice response per l'avvio senza l'accesso utente.
L'avvio senza l'accesso significa che non è necessario modificare la password prima di accedere a Windows.
3. Viene visualizzata la finestra di dialogo di accesso a Windows. Inserire la password di Windows in questa finestra di dialogo.
Si è ora connessi a Windows.
4. Il contatore del numero massimo di tentativi di immissione della password viene reimpostato.

Nota: È possibile anche richiedere un codice response con accesso utente. In questo caso viene chiesto di modificare le proprie credenziali Windows prima di accedere a Windows.

8.6.2 L'utente ha dimenticato la password

Si consiglia di eseguire le seguenti procedure per il recupero di una password dimenticata. Utilizzando una di queste procedure si evita che la password venga reimpostata centralmente:

- Utilizzare Local Self Help. Il recupero tramite Local Self Help permette di visualizzare la password corrente, consentendo di utilizzarla nuovamente senza doverla reimpostare o senza dover ricorrere all'helpdesk per assistenza. Per ulteriori informazioni, [vedere Recupero tramite Local Self Help](#) a pagina 29.
- Quando si esegue la procedura di Challenge/Response: Chiedere all'helpdesk di generare un codice response con accesso utente e di visualizzare la propria password durante una procedura Challenge/Response. Ciò consente di evitare la reimpostazione della password. È possibile continuare a lavorare con la vecchia password, per poi cambiarla solo in un secondo tempo.

Se non si esegue nessuna di queste procedure, fare quanto descritto di seguito:

1. Se si è dimenticata la password, si riceverà un codice response per l'avvio del computer con l'accesso utente. In tal caso sarà necessario modificare la password quando si effettua l'accesso a Windows (a condizione che il dominio sia accessibile).
2. Dopo aver modificato la password, utilizzare la nuova password per accedere all'Autenticazione all'accensione.

8.6.3 Token perso o dimenticato

In questo caso è necessaria la procedura Challenge/Response con accesso utente.

1. Viene richiesto di modificare la password durante la procedura Challenge/Response.

Nota: La finestra di dialogo per la modifica della password viene visualizzata solo se è stata stabilita una connessione al controller di dominio.

2. Se è obbligatorio l'accesso con token e PIN, si può decidere se modificare la password o se saltare la modifica della password, cliccando su **Annulla**.

■ L'utente ha dimenticato il token

Saltare la modifica della password cliccando su **Annulla** nella relativa finestra di dialogo, ha senso soltanto se si è momentaneamente dimenticato il token, ma in futuro lo si desidera utilizzare per effettuare l'accesso. Se si clicca su **Annulla**, si accede al sistema e si può riprendere il lavoro al computer.

Senza un token è possibile accedere soltanto tramite Challenge/Response durante l'Autenticazione all'accensione. Se si ritrova il token, è possibile utilizzarlo per accedere durante l'Autenticazione all'accensione.

■ L'utente ha perso il token

Se il token è stato perso, inserire una nuova password nella finestra di dialogo per la modifica della password. Con questa password viene effettuato l'accesso a Windows. Se i criteri nel proprio computer lo consentono (l'accesso con token durante l'Autenticazione all'accensione non è obbligatorio), è possibile accedere tramite l'Autenticazione all'accensione utilizzando questa password.

L'utilizzo non autorizzato del token da parte di qualsiasi utente che ne entri in possesso verrà bloccato. Gli utenti non autorizzati non possono utilizzare il token per l'accesso, anche se sono a conoscenza del PIN, poiché la password è stata modificata.

8.6.4 L'utente ha dimenticato il PIN

1. Se si è dimenticato il PIN del token, l'utente deve richiedere un codice response e inserire una nuova password. Con questa password viene effettuato l'accesso a Windows. È possibile utilizzarla anche per effettuare l'accesso tramite Autenticazione all'accensione, se autorizzati ad accedere utilizzando una password.
2. Un responsabile della protezione deve assegnare al token un nuovo PIN e memorizzarvi le nuove credenziali. È quindi possibile utilizzarlo ogni qual volta si desidera eseguire l'accesso.

8.6.5 Impossibile accedere al computer

Se non è più possibile accedere al computer, è possibile che l'autenticazione all'accensione sia danneggiata. Persino in una situazione così critica, SafeGuard Enterprise offre una procedura di richiesta/risposta con assistenza helpdesk, la quale consente di recuperare l'accesso alle unità cifrate. In questo caso la procedura di richiesta/risposta viene eseguita mediante un ambiente

WinPE. Se ci si trova ad affrontare una situazione talmente critica, si consiglia di contattare l'helpdesk di SafeGuard Enterprise. L'addetto all'helpdesk fornirà all'utente i file necessari e lo guiderà nei vari passaggi, al fine di recuperare l'accesso al computer.

8.7 Challenge/Response per utenti non in linea

Quando si utilizza la procedura Challenge/Response per utenti non in linea, è necessario tenere in considerazione alcuni aspetti particolari. Per gli utenti non in linea (ovvero gli utenti che non sono connessi al controller di dominio, per esempio responsabili alle vendite che lavorano dai loro notebook) non è possibile eseguire la modifica automatica della password durante la procedura Challenge/Response.

8.7.1 Challenge/Response per utenti non in linea con modalità di accesso nome utente/password

Esempio:

Si supponga di lavorare non in linea (ovvero non si è connessi al controller di dominio) e di avere dimenticato la password. Tramite la procedura Challenge/Response è possibile riacquistare rapidamente l'accesso al proprio computer.

Durante la procedura Challenge/Response, SafeGuard Enterprise consente anche di accedere automaticamente a Windows. Tuttavia, poiché una volta eseguita questa procedura non si è a conoscenza della password, si dovrebbe ripeterla ogni volta che si avvia il computer. Inoltre non sarebbe possibile sbloccare il computer nel caso in cui questo fosse bloccato (ad esempio, se è attivata una funzione di blocco sullo screen saver). In questo caso sarebbe necessario riavviare il computer, rischiando di perdere dati, e avviare nuovamente una procedura Challenge/Response.

Nota: Per questo motivo SafeGuard Enterprise offre la possibilità di visualizzare la password durante una procedura Challenge/Response. Gli utenti non in linea dovrebbero visualizzare la propria password durante una procedura Challenge/Response. Informare il responsabile dell'help desk che si desidera visualizzare la propria password. Il responsabile dell'help desk deve attivare esplicitamente la visualizzazione della password prima di generare il codice response.

Procedere come di seguito:

1. Per dare inizio la procedura Challenge/Response, cliccare su **Recupero** nella finestra di dialogo dell'Autenticazione all'accensione.
2. Chiamare l'help desk e comunicare il codice challenge.
3. Informare il responsabile dell'help desk che si desidera avviare il computer con l'accesso utente e che la password deve essere visualizzata.
4. Nella finestra di dialogo **Challenge/Response**, cliccare su **Avanti** e inserire il codice response.
5. Cliccare su **OK**.

Verrà chiesto se la vecchia password deve essere visualizzata sullo schermo.

6. Scegliere **SÌ** e cliccare su **OK**.

7. La finestra di dialogo successiva informa che la password verrà visualizzata premendo **Invio**, sulla **Barra spaziatrice**, o cliccando sul testo.

Nota: NON cliccare su **OK**. Dopo aver cliccato su **OK** il processo di avvio continuerà infatti **SENZA** che la password venga visualizzata.

La password viene visualizzata per 5 secondi. In seguito, il processo di avvio continua automaticamente.

8. Premere **Invio**, la **Barra spaziatrice**, oppure cliccare sul testo.

Viene visualizzata la password.

Nota: Assicurarsi che nessun utente non autorizzato possa vedere, involontariamente o volontariamente, il contenuto della schermata. È possibile nascondere immediatamente la propria password, premendo la **Barra spaziatrice**, **Invio**, oppure cliccando sulla finestra blu. La password viene mostrata per un intervallo di tempo massimo di 5 secondi.

9. È possibile leggere la password e utilizzarla per l'accesso durante l'Autenticazione all'accensione e per l'accesso a Windows.

È quindi possibile riprendere il lavoro al computer.

8.7.2 Challenge/Response per utenti non in linea con modalità di accesso "solo token"

In questo caso, se il PIN o il token sono stati dimenticati, o se quest'ultimo è andato perduto, la procedura da utilizzare varia se si è a conoscenza o meno delle proprie credenziali Windows.

- ❖ Si è a conoscenza delle proprie credenziali Windows

- a) Se si conoscono le credenziali Windows, iniziare la procedura Challenge/Response come descritto. L'utente viene automaticamente connesso a Windows.

La modalità di accesso **Solo token** viene reimpostata per la durata della sessione di lavoro a seguito della procedura Challenge/Response. Di conseguenza sarà possibile anche accedere a Windows utilizzando il proprio nome utente e la password.

Se il computer è bloccato, sarà quindi possibile sbloccarlo immettendo la password di Windows. L'accesso durante l'Autenticazione all'accensione, tuttavia, è possibile solo tramite Challenge/Response.

- ❖ Non si è a conoscenza delle proprie credenziali Windows

- a) Se non si è a conoscenza delle proprie credenziali Windows e si è dimenticato il PIN, è possibile iniziare anche in questo caso una procedura Challenge/Response durante la quale verrà visualizzata la password.

- b) Informare il responsabile dell'help desk che la password deve essere visualizzata.

Poiché la modalità di accesso **Solo token** sarà disattivata, è possibile anche sbloccare il computer, se bloccato, utilizzando questa password.

L'accesso durante l'Autenticazione all'accensione, tuttavia, è possibile solo tramite Challenge/Response.

9 Icona dell'area di notifica e descrizione comandi

È possibile accedere senza difficoltà a tutte le funzioni importanti del client di SafeGuard Enterprise disponibili nel computer. L'icona dell'area di notifica di SafeGuard Enterprise sulla barra delle applicazioni di Windows consente di accedere a queste funzioni.

Nota: Il funzionamento dell'icona nell'area di notifica è definito dal responsabile della protezione, il quale specifica, impostando un apposito criterio, se l'icona viene visualizzata o meno sul computer. L'Icona può anche essere impostata in modalità "silenziosa". In questo caso non vengono visualizzati messaggi sotto forma di fumetto.

L'icona dell'area di notifica consente di visualizzare informazioni o di eseguire determinate azioni. Se si fa clic sull'icona con il pulsante destro del mouse, viene visualizzato un menu contenente le seguenti voci:

- **Visualizza:**
 - **Gruppo di chiavi:** Mostra tutte le chiavi disponibili.
 - **Certificato:** Mostra le informazioni relative al proprio certificato.
 - **Crea nuova chiave:** Apre una finestra di dialogo per la creazione di una nuova chiave da utilizzare per lo scambio di dati mediante supporti rimovibili ([vedere SafeGuard Data Exchange](#) a pagina 53).
 - **Local Self Help**

Se Local Self Help è attivato per il computer in uso mediante il relativo criterio, il comando Local Self Help viene mostrato nel menu di scelta rapida dell'icona dell'area di notifica. Mediante questo comando è possibile avviare la procedura guidata di Local Self Help. Local Self Help è una modalità di recupero dell'accesso per cui non è richiesto l'intervento dell'helpdesk. Per ulteriori informazioni, [vedere Recupero tramite Local Self Help](#) a pagina 29.
 - **Cambia passphrase supporto:** Apre una finestra di dialogo per la creazione di una nuova chiave da utilizzare per lo scambio di dati mediante supporti rimovibili ([vedere SafeGuard Data Exchange](#) a pagina 53).
 - **Sincronizza:** Avvia la sincronizzazione dei dati con SafeGuard Enterprise Server. Lo stato di avanzamento e il risultato della sincronizzazione vengono visualizzati nella descrizione comandi.
- Nota:** È possibile avviare la sincronizzazione anche facendo doppio clic sull'icona dell'area di notifica.
- **Stato:** Apre una finestra di dialogo che fornisce informazioni sullo stato corrente del computer protetto da SafeGuard Enterprise:

Campo	Informazioni
Ultimo criterio ricevuto	Mostra la data e l'ora di ricezione dell'ultimo criterio.

Campo	Informazioni
Ultima chiave ricevuta	Mostra la data e l'ora di ricezione dell'ultima chiave.
Ultimo certificato ricevuto	Mostra la data e l'ora di ricezione dell'ultimo certificato.
Ultimo contatto server	Mostra la data e l'ora dell'ultimo contatto con il server.
Stato utente SGN	<p>Mostra lo stato dell'utente che ha eseguito l'accesso al computer (accesso a Windows):</p> <ul style="list-style-type: none"> <p>■ In sospeso</p> <p>La replica dell'utente mediante l'Autenticazione all'accensione è in sospeso, ad esempio la sincronizzazione iniziale dell'utente non è stata ancora completata. Questa informazione è particolarmente importante dopo che si è effettuato il primo accesso a SafeGuard Enterprise, in quanto è possibile accedere mediante l'Autenticazione all'accensione soltanto dopo che è stata completata la sincronizzazione dei dati dell'utente.</p> <p>■ Utente SGN</p> <p>L'utente è stato assegnato all'installazione di SafeGuard Enterprise come utente SafeGuard Enterprise.</p> <p>■ Guest SGN</p> <p>L'utente che ha eseguito l'accesso a Windows è un utente guest SafeGuard Enterprise. All'utente è consentito accedere a Windows senza essere assegnato al computer protetto da SafeGuard Enterprise come utente SafeGuard Enterprise.</p> <p>■ Guest SGN - account di servizio</p> <p>L'utente che ha eseguito l'accesso a Windows è un utente guest SafeGuard Enterprise che ha effettuato l'accesso utilizzando un account di servizio per le attività amministrative.</p> <p>■ Sconosciuto</p> <p>Indica che non è possibile determinare lo stato dell'utente.</p>
Stato della cache locale Pacchetti di dati preparati per la trasmissione	Indica se sono presenti pacchetti da inviare al server Sophos SafeGuard.
Stato Local Self Help (LSH)	Indica se Local Self Help è stato abilitato all'interno di un criterio, e se è stato attivato sul computer

Campo	Informazioni
Abilitato Attivo	dall'utente. Per ulteriori informazioni, vedere Recupero tramite Local Self Help a pagina 29.
Pronto per modifica del certificato	Questa dicitura viene visualizzata, se il responsabile della protezione ha assegnato al computer un nuovo certificato per l'accesso con token di cifratura. È ora possibile modificare il certificato per accesso tramite token, vedere Modifica del certificato per l'accesso con token di cifratura a pagina 12.

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

10 Accesso alle funzioni mediante estensioni di Esplora risorse

È possibile accedere alle funzioni per la cifratura dalle rispettive voci dei menu di scelta rapida in Esplora risorse.

10.1 Estensioni Explorer per la cifratura basata su file

È possibile accedere alle funzioni per la cifratura basata su file tramite le rispettive voci dei menu di scelta rapida in Windows Explorer. Le funzioni sono disponibili nei menu di scelta rapida di

- volumi
- supporti rimovibili
- directory
- file

La voce **Cifratura file** è stata aggiunta al menu di scelta rapida. Da questo menu, è possibile accedere alle singole funzioni.

Se al volume selezionato non è applicabile alcun criterio di cifratura basata su file, è possibile solamente determinare lo stato della cifratura e visualizzare la finestra di dialogo per la generazione di nuove chiavi dal menu di scelta rapida.

Se al volume, supporto rimovibile, directory o file selezionato è stato applicato un criterio di cifratura basata su file, al menu di scelta rapida vengono aggiunte voci relative alla cifratura.

Nota: Le funzioni visualizzate variano a seconda delle impostazioni definite nei criteri. Dipendono anche dalla disponibilità o meno della relativa funzione per il volume selezionato. L'ambito delle funzioni varia a seconda che per il volume interessato sia stata utilizzata la cifratura basata su file o basata su volume.

Sono disponibili le seguenti funzioni:

- **Avvia cifratura:** Se si sceglie questa opzione dal menu di scelta rapida di un volume, tutti i file possono essere cifrati o cifrati di nuovo.
- **Mostra stato della cifratura:** Indica se un volume, un supporto rimovibile o un file è stato cifrato; specifica la chiave utilizzata, se tale chiave è inclusa nel gruppo di chiavi dell'utente e se è possibile accedere a questo file.
- **Decifrazione:** Consente di decifrare il volume o il file selezionato.
- **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.
- **Gestione chiavi: Crea nuova chiave:** Consente di aprire una finestra di dialogo per la creazione di chiavi locali definite dall'utente.

10.2 Estensioni Explorer per la cifratura basata su volume

Al menu di scelta rapida di Windows Explorer è stata aggiunta la voce **Cifratura**.

Se il volume è cifrato, accanto alla voce di menu viene visualizzato un simbolo a forma di chiave. Se viene visualizzata una chiave verde si dispone delle chiavi necessarie per accedere al volume.

Nota: **Cifratura file>Mostra stato di cifratura** visualizza lo stato di cifratura dei file sul volume, dal punto di vista di una cifratura basata su file. I file presenti su un volume cifrato possono venire cifrati anche in modalità basata su file. In questo caso, verrà visualizzata la relativa finestra di dialogo.

Aggiungi/rimuovi chiavi

È possibile aggiungere/rimuovere chiavi al/dal volume cifrato, se le impostazioni specificate nei criteri applicati lo consentono. In tal modo si consente a tutti i proprietari della relativa chiave di accedere ai dati cifrati su questo volume.

È possibile assegnare chiavi al volume tramite la finestra di dialogo **Proprietà** del volume. Questa finestra di dialogo contiene la scheda **Cifratura** (cliccare col tasto destro del mouse su **Volume>Proprietà >Cifratura**).

Selezionare una chiave dall'elenco inferiore e cliccare su **Aggiungi chiave**. Il file viene spostato verso l'alto dall'elenco di selezione delle chiavi. È incluso nell'elenco di chiavi che possono essere utilizzate per accedere al volume cifrato.

Utilizzando l'opzione **Rimuovi chiave** è possibile rimuovere la chiave dall'elenco di chiavi utilizzate per accedere ai supporti.

11 Cifratura dei dati

SafeGuard Enterprise cifra i dati in un computer basandosi su volumi oppure su file. Il responsabile della protezione definisce nei criteri di protezione i volumi (le unità) da cifrare.

11.1 Cifratura trasparente

I file presenti su un'unità cifrata vengono cifrati in maniera trasparente. Non vengono visualizzati messaggi di avviso per la cifratura o la decifrazione quando l'utente apre, modifica e salva i file. Quando si aprono i file, questi vengono decifrati ed è quindi possibile modificarli. Al momento della chiusura o del salvataggio, i file vengono nuovamente cifrati.

Se si copiano o si spostano file (anche mediante il comando **Salva con nome**) da un'unità cifrata a un percorso non cifrato nel computer, i file vengono decifrati. I file vengono memorizzati nel nuovo percorso in formato di testo normale.

11.2 Cifratura iniziale

La cifratura iniziale dei computer protetti da SafeGuard Enterprise può comportare la creazione di criteri di cifratura da distribuire ai computer all'interno di un pacchetto di configurazione.

Una volta avvenuta la distribuzione ai computer del primo criterio di cifratura, viene avviata la procedura iniziale di cifratura secondo le impostazioni del criterio ricevute.

11.2.1 Cifratura iniziale per la cifratura basata su volume

Terminata l'installazione di SafeGuard Enterprise, non appena il computer riceve un criterio per la cifratura basata su volume, questo tipo di cifratura viene avviato automaticamente.

La cifratura iniziale basata su volume viene eseguita nello sfondo, consentendo, in questo modo, di continuare a utilizzare il computer.

11.2.2 Cifratura iniziale per la cifratura basata su file

Se un criterio che prevede la cifratura dei file viene applicato a un percorso del computer, in Esplora risorse viene visualizzato un simbolo a forma di chiave gialla accanto ai file interessati.

La chiave gialla da sola non indica necessariamente che tutti i file presenti nell'unità siano già stati cifrati. Innanzitutto deve essere eseguita una cifratura iniziale.

Se è prevista la cifratura dei file, la cifratura iniziale può essere avviata automaticamente o manualmente.

11.2.3 Restrizioni della cifratura iniziale dei computer protetti da SafeGuard Enterprise

La cifratura iniziale dei computer protetti da SafeGuard Enterprise può comportare la creazione di criteri di cifratura da distribuire ai computer all'interno di un pacchetto di configurazione. Se il client SafeGuard Enterprise non viene connesso a un server SafeGuard Enterprise subito dopo l'installazione del pacchetto di configurazione e, al contrario, risulta essere

temporaneamente non in linea, solo i criteri di cifratura con le seguenti impostazioni specifiche saranno immediatamente attivi nel computer protetto da SafeGuard Enterprise:

- Protezione del dispositivo basata su volume utilizzando la **Chiave del computer definita** come chiave di cifratura

Per tutti gli altri criteri che comportano l'attivazione della cifratura mediante le chiavi definite dall'utente nel computer protetto da SafeGuard Enterprise, il relativo pacchetto di configurazione deve essere riassegnato al computer. Le chiavi definite dall'utente verranno dunque create solo dopo che il client SafeGuard Enterprise viene nuovamente connesso al server SafeGuard Enterprise.

Ciò è dovuto al fatto che la **Chiave del computer definita** viene creata nel computer protetto da SafeGuard Enterprise al primo riavvio dopo l'installazione, mentre le chiavi definite dall'utente possono essere create nel computer soltanto dopo che questo è stato registrato nel server SafeGuard Enterprise.

11.3 Cifratura basata su volume

Se il responsabile della protezione ha definito un criterio appropriato, la cifratura basata su volume per un disco del computer protetto da SafeGuard Enterprise viene avviata automaticamente.

1. Viene visualizzata una finestra di dialogo in cui viene richiesto di selezionare una chiave che consente di accedere al volume.

Nota: Tutti gli utenti il cui gruppo di chiavi include questa chiave potranno accedere a questo volume. Il responsabile della protezione definisce l'ambito delle chiavi fornite. Se il responsabile della protezione ha definito una chiave specifica, non sarà possibile selezionare una chiave.

2. Cliccare su **OK** per avviare la cifratura.

Durante il processo di cifratura, un Visualizzatore cifratura mostra lo stato di avanzamento della cifratura del volume da cifrare. Se presenti, mostra anche i volumi già cifrati. Il Visualizzatore cifratura è presente, ridotto a icona, sulla barra delle applicazioni di Windows. Può essere aperto cliccando sulla relativa icona. Se si desidera che il Visualizzatore cifratura rimanga ridotto a icona, è possibile richiedere la visualizzazione di una notifica quando la cifratura è stata completata, attivando l'opzione **Visualizza notifica prima della chiusura**. Il visualizzatore viene chiuso automaticamente al completamento della cifratura. Il volume cifrato può essere utilizzato normalmente come qualsiasi altro volume presente non cifrato presente nel computer.

Nota:

Nei sistemi Windows 7 Professional, Enterprise e Ultimate, viene creata una partizione di sistema sui computer endpoint, senza l'assegnamento di una lettera di unità. Tale partizione non può essere cifrata con SafeGuard Enterprise.

11.4 Cifratura basata su file

La cifratura di un volume viene avviata automaticamente oppure il processo viene avviato manualmente dall'utente.

1. Se la cifratura non viene attivata automaticamente, selezionare **Cifratura file > Avvio cifratura**.
2. Se il responsabile della protezione non ha definito una chiave specifica, in entrambi i casi verrà visualizzata una finestra di dialogo in cui è richiesto di selezionare una chiave che consenta di accedere al volume.

Nota:

Tutti gli utenti il cui gruppo di chiavi include questa chiave potranno accedere a questo volume. Il responsabile della protezione definisce l'ambito delle chiavi fornite. Se il responsabile della protezione ha definito una chiave specifica, non sarà possibile selezionare una chiave.

Per lo scambio di dati con utenti che dispongono di SafeGuard Enterprise installato nel computer, ma che non utilizzano la stessa chiave dell'utente che invia i dati, in genere sono richieste **chiavi locali generate dagli utenti**. 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 attivata l'opzione **Crittografare nuovamente i file se sono già stati crittografati con una chiave diversa**, i file cifrati per i quali esiste una chiave verranno decifrati e nuovamente cifrati utilizzando la nuova chiave.

3. Selezionare una chiave, quindi cliccare su **OK**.

Tutti i dati del volume interessato sono cifrati.

11.4.1 Definizione di una chiave predefinita

Definendo una chiave predefinita si specifica la chiave da utilizzare per la cifratura durante l'esecuzione di operazioni.

1. È possibile definire la chiave predefinita tramite il menu di scelta rapida di un file presente su un volume, o dal menu di scelta rapida del supporto rimovibile.
2. Selezionare **Cifratura file>Imposta chiave predefinita** per visualizzare la finestra di dialogo per la selezione della chiave.

La chiave selezionata viene utilizzata per tutti i processi di cifratura successivi sul volume.

3. Se si desidera utilizzare una chiave diversa, basta semplicemente definire una nuova chiave predefinita.

11.4.2 Stato di cifratura

Nei volumi cifrati in modalità basata su file, i singoli file vengono contrassegnati con simboli di chiave di diversi colori. I colori della chiave indicano lo stato di cifratura.

- **Chiave verde:** il file è cifrato ed è possibile accedervi.
- **Chiave grigia:** al file è stato applicato un criterio di cifratura. Tuttavia il file non è stato ancora cifrato.
- **Chiave rossa:** il file è cifrato con una chiave che non è inclusa nel gruppo di chiavi dell'utente. Non è possibile accedervi.

È possibile visualizzare lo stato di cifratura di un file tramite il relativo menu di scelta rapida. Selezionando **Cifratura file >Mostra stato di cifratura**, è possibile aprire una finestra contenente lo stato di cifratura.

Se si seleziona **Cifratura file >Stato di cifratura** dal menu di scelta rapida del volume stesso, verrà visualizzata una finestra di dialogo contenente tutti i file e il relativo stato di cifratura.

11.5 Restrizioni di accesso ai volumi

SafeGuard Enterprise nega l'accesso ai volumi nei seguenti casi:

Volumi per cui la cifratura non è riuscita

Se è presente un criterio che stabilisce che un volume o tipo di volume deve essere cifrato e non è possibile eseguirne la cifratura, l'accesso a tale volume viene negato.

Se si tenta di accedere al volume, viene visualizzato il relativo messaggio.

Oggetti del file system non identificati

Gli oggetti del file system non identificati sono volumi che non possono essere identificati in modo distinto come formato testo normale o come cifrati da SafeGuard Enterprise.

Se è presente un criterio che stabilisce che un volume di questo tipo deve essere cifrato e non è possibile eseguirne la cifratura, viene negato l'accesso a tale volume. Se si tenta di accedere al volume, viene visualizzato il relativo messaggio.

Se non è presente alcun criterio di cifratura per un oggetto del file system non identificato, sarà possibile accedere al volume.

12 SafeGuard Data Exchange

SafeGuard Data Exchange consente di cifrare i dati memorizzati su supporti rimovibili collegati al computer e scambiare dati con altri utenti. Tutti i processi di cifratura e decifrazione vengono eseguiti in modo trasparente e richiedono un minimo di interazione con l'utente.

Solo gli utenti che dispongono delle chiavi adeguate possono leggere il contenuto dei dati cifrati. Tutti i successivi processi di cifratura vengono eseguiti in modo trasparente. Cifratura trasparente significa che i dati che sono stati cifrati e salvati vengono automaticamente decifrati da un'applicazione al momento del successivo accesso.

Una volta salvati, i file vengono nuovamente cifrati automaticamente. 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.

Nota: Il funzionamento di SafeGuard Data Exchange sul computer è definito in modo centralizzato dal responsabile della protezione.

Nell'amministrazione centralizzata, 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 sul dispositivo vengono inizialmente cifrati. Inoltre, 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 esegue 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 di conseguenza 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 che siano disponibili a entrambi gli utenti oppure creare una nuova chiave. Se si genera una nuova chiave, è necessario fornire al destinatario dei dati la passphrase per la chiave.
- **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.

12.1 Impostazioni per la gestione di supporti rimovibili

Se SafeGuard Data Exchange è installato nel computer, i supporti rimovibili verranno gestiti in base alle impostazioni predefinite configurate dal responsabile della protezione. Un responsabile della protezione può definire le seguenti impostazioni per SafeGuard Data Exchange (si noti che è possibile anche una combinazione di varie impostazioni):

- **Cifratura iniziale di tutti i file:** In questo caso la cifratura di tutti i dati presenti su un supporto rimovibile viene avviata non appena si collega il dispositivo al computer. Questa impostazione garantisce che i supporti rimovibili contengano esclusivamente dati cifrati. Quando si avvia la cifratura, viene chiesto di selezionare una chiave oppure viene utilizzata una chiave predefinita.
- **È consentito annullare la cifratura iniziale:** Quando viene avviata la cifratura iniziale, viene visualizzata una finestra di dialogo che consente di annullarla.
- **Non è consentito accedere ai dati non cifrati:** In questo caso SafeGuard Data Exchange accetterà solo dati cifrati su supporti rimovibili. Se sui supporti rimovibili sono presenti dati non cifrati, il sistema non ne consentirà l'accesso. Sarà possibile accedere a questi dati solo dopo la loro cifratura.

- **È consentito decifrare i file:** In questo caso è possibile decifrare esplicitamente i file presenti sui supporti rimovibili. Un file che è stato esplicitamente decifrato rimane in formato testo normale sul supporto rimovibile, se, ad esempio, viene trasferito a terze parti.
- **È possibile definire una passphrase dei supporti per i supporti rimovibili:** La prima volta che si connette un supporto rimovibile, viene richiesto di immettere una passphrase dei supporti.
- **Cartella di testo normale sui supporti rimovibili:** Il responsabile della protezione può definire un cartella di testo normale che verrà creata su tutti i supporti rimovibili. I file contenuti in questa cartella non sono cifrati da SafeGuard Data Exchange.
- **È consentito annullare la cifratura iniziale:** 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.

12.2 Passphrase dei supporti singola per tutti i dispositivi rimovibili collegati al computer

SafeGuard Data Exchange consente di definire una passphrase dei supporti unica, che fornisca accesso a tutti i dispositivi rimovibili connessi al computer. Questa è 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 dei supporti. La passphrase del supporto è connessa ai computer cui è possibile accedere. Ciò significa che viene utilizzata la stessa passphrase del supporto per tutti i computer.

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

Una passphrase dei supporti risulta utile nei seguenti scenari:

- Se si desidera utilizzare dati cifrati su supporti rimovibili su 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.

Inoltre, è 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.

Nota: 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:

- Chiavi USB
- Dischi rigidi esterni collegati tramite USB o FireWire
- Unità CD RW (UDF)
- Unità DVD RW (UDF)
- FireWire
- Schede di memoria nei lettori di schede USB (incluse ZIP, JAZ)

12.3 Cifratura di supporti rimovibili

12.3.1 Cifratura iniziale

La cifratura dei dati non cifrati presenti su 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 abilitati 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 **Cifratura file** > **Avvia cifratura** dal menu di scelta rapida del supporto 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, quindi 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 viene utilizzata per la cifratura iniziale dei dispositivi rimovibili collegati ai computer in un secondo momento.

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 di supporto. 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 attivata l'opzione **Cifrare i file in formato testo e aggiornare i file cifrati**, i file cifrati con una chiave esistente verranno decifrati e nuovamente cifrati utilizzando la nuova chiave.

Timeout della cifratura iniziale

Se la cifratura iniziale è configurata per l'avvio automatico, è possibile avere il diritto di annullare la cifratura iniziale. In questo caso il pulsante **Annulla** è attivato, viene visualizzato

un pulsante **Avvia**, e l'inizio del processo di cifratura viene ritardato di 30 secondi. Se non si seleziona **Annulla** durante questo intervallo di tempo, la cifratura iniziale verrà automaticamente avviata dopo 30 secondi. Se si seleziona **Avvia**, la cifratura iniziale viene avviata immediatamente.

Cifratura iniziale per utenti con passphrase dei supporti

Se l'utilizzo di una passphrase dei supporti è stato definito in un criterio, viene richiesto di immettere la passphrase dei supporti prima della cifratura iniziale. La passphrase dei supporti è valida per tutti i supporti rimovibili ed è associata al computer o a tutti i computer per i quali si dispone di diritto di accesso.

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

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

Nota: La cifratura iniziale non viene avviata nei computer in cui non è stata impostata la passphrase dei dispositivi.

12.3.2 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 decifrazione vengono 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.

Nota: 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 alla nuovo percorso è applicato un criterio di cifratura diverso, i dati vengono cifrati in base a tale criterio.

Passphrase dei supporti

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 di una 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 alla 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.

Cambia/reimposta passphrase dei supporti

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

Se la passphrase dei supporti è stata dimenticata, 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. Selezionare quindi **Modifica passphrase dei supporti** dal menu dell'icona dell'area di notifica. All'utente viene comunicato che non sono presenti passphrase dei supporti nel computer ed è quindi necessario immetterne una nuova.

Sincronizzazione della passphrase dei supporti

La passphrase dei supporti presente nei dispositivi e nel computer verrà sincronizzata automaticamente. Se si cambia la passphrase dei supporti nel computer e si connette un dispositivo in cui è ancora in uso la versione precedente della passphrase, all'utente verrà comunicato che le passphrase dei supporti sono state sincronizzate. Questo vale per tutti i computer a cui è consentito l'accesso.

Nota: 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).

Definizione di una chiave predefinita

Definendo una chiave predefinita si specifica la chiave da utilizzare per la cifratura durante l'esecuzione di operazioni ordinarie.

È possibile definire la chiave predefinita tramite il menu di scelta rapida di un file presente su un supporto rimovibile o tramite il menu di scelta rapida del supporto rimovibile stesso. È inoltre possibile impostare immediatamente una chiave come chiave predefinita, quando si crea una nuova chiave locale nella finestra di dialogo **Crea chiave**.

Selezionare **Cifratura file > Imposta chiave predefinita** Imposta chiave predefinita per aprire una finestra di dialogo o per selezionare la chiave.

La chiave selezionata in questa finestra di dialogo viene utilizzata per tutti i processi di cifratura successivi eseguiti su tale supporto rimovibile di archiviazione. Se si desidera utilizzarne una diversa, è possibile definire una nuova chiave predefinita in qualsiasi momento.

Nel criterio è possibile specificare una chiave predefinita da utilizzare per la cifratura. Se non è definita nel criterio, all'utente viene richiesto di specificare una chiave predefinita iniziale.

12.4 Scambio di dati mediante 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, 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**

Per gli utenti che non dispongono di SafeGuard Enterprise installato nel computer è disponibile SafeGuard Portable. Anche per lo scambio di dati con SafeGuard Portable è necessario utilizzare chiavi locali in combinazione con una passphrase.

In aggiunta, SafeGuard Portable deve essere copiato sul supporto di memorizzazione rimovibile. È inoltre necessario fornire la passphrase al destinatario dei dati cifrati. Utilizzando la passphrase e SafeGuard Portable, il destinatario può decifrare i file cifrati e, ad esempio, modificarli, quindi salvarli nuovamente in forma cifrata sul supporto rimovibile. Poiché SafeGuard Portable è un'applicazione autonoma, per poter accedere ai dati cifrati non è necessario installare alcun software aggiuntivo.

Nota: Il responsabile della protezione stabilisce nel criterio di protezione relativo all'utente se SafeGuard Portable debba venire copiato sui supporti rimovibili o meno.

12.4.1 Importazione di chiavi da un file

Se si ricevono supporti rimovibili contenenti dati che sono stati cifrati 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 desiderato nel dispositivo rimovibile, e cliccare su **Cifatura file > Gestione chiavi > Importa chiave**.
2. Inserire la passphrase nella finestra di dialogo visualizzata.

La chiave viene importata ed è possibile accedere al file.

12.4.2 Creazione di chiavi locali

1. Cliccare con il tasto destro del mouse sull'icona di Sophos SafeGuard nell'area di notifica, nella barra delle applicazioni di Windows.
2. Cliccare su **Crea nuova chiave**.
3. Nella finestra di dialogo **Crea chiave**, inserire **Nome** e **Passphrase** della chiave.

Il nome interno della chiave è visualizzato nel campo in basso.

4. Confermare la passphrase.

Se si immette 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 la 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. Mediante l'opzione **Utilizza come nuova chiave predefinita per l'unità**, è possibile impostare la nuova chiave immediatamente come chiave predefinita per l'unità visualizzata.

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 saranno stati sincronizzati con il server SafeGuard Enterprise.

Se tale chiave viene impostata come predefinita, tutti dati i copiati su supporti rimovibili 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 supporto di memorizzazione rimovibile utilizzando la chiave creata localmente. A tale scopo, selezionare **Cifratura file > Avvia cifratura** 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.

12.5 Scrittura di file su CD mediante la Masterizzazione guidata CD di Windows

Nota:

In Windows XP, con la Masterizzazione guidata CD di Windows, è possibile scrivere file soltanto su CD. Windows XP non supporta la masterizzazione di file su DVD tramite la Masterizzazione guidata CD di Windows.

SafeGuard Data Exchange consente di scrivere file cifrati su CD tramite la Masterizzazione guidata CD di Windows.

Per eseguire questa operazione, è necessario specificare una regola di cifratura per l'unità di registrazione dei CD. SafeGuard Data Exchange aggiunge una finestra di dialogo alla Masterizzazione guidata CD. In questa finestra è possibile specificare in che modo i file vengono masterizzati sul CD (cifrati o formato testo).

Nota: Se per l'unità di registrazione CD non esistono regole di cifratura, i file vengono masterizzati sul CD in formato testo normale. La finestra SafeGuard Data Exchange, nella quale è possibile specificare lo stato di cifratura dei file da masterizzare sul CD, non viene visualizzata.

Dopo aver inserito il nome del CD, viene visualizzata l'estensione masterizzazione disco SafeGuard® Enterprise.

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 fra 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 trovare i relativi file 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 **Cifrare 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 vengono prima decifrati e poi masterizzati sul CD.

Copia di SafeGuard Portable su supporti ottici

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

12.5.1 Masterizzazione di CD/DVD con Windows Vista e Windows 7

Windows Vista e Windows 7 forniscono la Masterizzazione guidata CD, per masterizzare CD e DVD.

SafeGuard Disc Burning Extension per la Masterizzazione guidata CD è disponibile solo per la masterizzazione di CD/DVD in formato **Mastered**. La procedura guidata viene visualizzata solo se i file stanno per essere scritti su 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.

12.6 SafeGuard Portable

Utilizzando SafeGuard Portable è possibile scambiare dati cifrati mediante supporti rimovibili con destinatari che non dispongono di SafeGuard Data Exchange installato nel computer. 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.

Nota: SafeGuard Portable cifra e decifra solamente i file cifrati con AES 256.

L'utilizzo di SafeGuard Portable in combinazione con la relativa 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 mediante quella specifica chiave. Il destinatario può decifrare i dati cifrati, e cifrarli nuovamente.

Nota: È necessario comunicare la passphrase dei supporti o la passphrase di una chiave locale al destinatario con il dovuto anticipo.

Il destinatario può utilizzare chiavi esistenti create da SafeGuard Data Exchange per la cifratura, oppure creare una nuova chiave 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. Il programma resta sul supporto rimovibile.

Nota: Se si è utenti di SafeGuard Enterprise, in genere non è necessario utilizzare SafeGuard Portable. La seguente descrizione riguarda gli utenti che non dispongono di SafeGuard Enterprise installato nel computer e che pertanto devono utilizzare SafeGuard Portable per modificare i dati cifrati.

12.6.1 Modifica di file utilizzando SafeGuard Portable

L'utente riceve supporti rimovibili contenenti 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 i dati cifrati presenti sui supporti rimovibili e cifrarli di nuovo. SafeGuard Portable fornisce funzionalità simili a quelle offerte in Windows Explorer.

Oltre a dettagli dei file già noti visualizzati in Windows Explorer (nome, dimensioni, ecc), in SafeGuard Portable è riportata 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.

Nota: È possibile decifrare i file soltanto se si è a conoscenza della chiave utilizzata.

- Per modificare file presenti sul supporto rimovibile, cliccare sul file desiderato e selezionare comando adeguato dal menu di scelta rapida (con un clic del tasto destro del mouse), oppure dal menu **File**.

I seguenti comandi sono disponibili dal menu di scelta rapida:

Imposta chiave di cifratura	Apri la finestra di dialogo Inserisci chiave . In questa finestra è possibile generare una chiave di cifratura tramite SafeGuard Portable.
Cifratura	Consente di cifrare il file selezionato sul supporto rimovibile. Per la cifratura viene scelta l'ultima chiave utilizzata.
Decifrazione	Aprire la finestra di dialogo Inserisci passphrase . Inserire la passphrase per la decifrazione del file selezionato in questa finestra di dialogo.
Stato della cifratura	Consente di visualizzare una finestra di dialogo che mostra lo stato della cifratura del file.
Copia in	Consente di copiare il file in una cartella di propria scelta e di decifrarlo.
Elimina	Consente di eliminare dal supporto rimovibile il file selezionato.

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

12.6.1.1 Impostazione delle chiave di cifratura

Per cifrare un file presente su un supporto rimovibile e creare una chiave di cifratura:

- Dal menu di scelta rapida o dal menu **File**, selezionare **Imposta chiave di cifratura**.
Viene visualizzata la finestra di dialogo **Inserisci chiave**.
- Inserire un **Nome** e una **Passphrase** per la chiave. **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 verrà utilizzata d'ora in poi per la cifratura.

12.6.1.2 Cifratura di file su supporti rimovibili

1. In SafeGuard Portable Explorer, selezionare il file e, tramite il menu di scelta rapida, cliccare su **Cifra**.

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

Quando si salvano nuovi file su supporto rimovibile utilizzando la procedura di trascinamento della selezione in SafeGuard Portable Explorer, viene richiesto se si desidera cifrarli.

In questo caso, se non è stata eseguita alcuna cifratura con SafeGuard Portable in precedenza, viene visualizzata una finestra di dialogo per l'impostazione della chiave. Inserire in tale finestra il nome della chiave e la passphrase (che deve essere confermata). Cliccare su **OK**.

2. Selezionare il file da cifrare con la chiave appena impostata e cliccare su **Cifra** dal menu di scelta rapida oppure dal menu **File**.

Il file viene cifrato e, completato il processo, viene visualizzato un relativo messaggio.

Nota: 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.

12.6.1.3 Decifrazione di file presenti in supporti rimovibili

1. Selezionare il file in SafeGuard Portable Explorer, quindi cliccare su **Decifra** dal menu di scelta rapida.

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 del supporto consente di accedere a tutti i file cifrati sul supporto rimovibile, indipendentemente dalla chiave locale utilizzata per cifrarli. Se si dispone solo della passphrase di una chiave locale, sarà possibile accedere solo 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 sul supporto rimovibile e immesso la passphrase della chiave, la prossima volta che si cifrano o si decifrano file cifrati con la stessa chiave, non sarà necessario immettere nuovamente la passphrase.

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.

Dopo la decifrazione, i file sono disponibili in formato testo normale sul supporto rimovibile. I file decifrati vengono nuovamente cifrati alla chiusura di SafeGuard Portable.

12.6.1.4 Cifratura di nuovi file utilizzando SafeGuard Portable

Utilizzando SafeGuard Portable, è anche possibile copiare i propri file su supporti rimovibili in forma già cifrata.

1. Spostare i file richiesti su SafeGuard Portable Explorer mediante il trascinamento della selezione.

Verrà chiesto se si desidera cifrare il file in questione.

2. Confermare che si desidera procedere alla cifratura. Il file viene cifrato con l'ultima chiave utilizzata e successivamente copiato sul supporto rimovibile.

12.6.1.5 Determinazione dello stato di cifratura di un file

1. Selezionare il file e fare clic su **Stato di cifratura**, dal menu di scelta rapida o dal menu **File**.

Lo stato di cifratura verrà anche indicato nella colonna **Chiave** accanto al nome del file in SafeGuard Portable Explorer.

12.6.2 Altre operazioni eseguibili tramite SafeGuard Portable

Sono disponibili anche le seguenti operazioni:

- ❖ **Apri:** Questo comando è disponibile solo nel menu **File** di SafeGuard Portable.

Quando si apre un file cifrato tramite questo comando di menu, viene richiesta l'inserimento della passphrase. Inserire la passphrase e cliccare su **OK**. Il file viene decifrato e aperto.

- ❖ **Elimina:** Elimina gli elementi selezionati.

- ❖ **Copia in:** Questo comando è disponibile solo nel menu di scelta rapida, accessibile mediante il tasto destro del mouse in SafeGuard Portable Explorer.

Il comando consente di copiare file da un supporto rimovibile a un'altra unità del computer.

- ❖ **Esci:** Questo comando è disponibile solo nel menu **File** di SafeGuard Portable.

Il comando **Esci** consente di chiudere SafeGuard Portable.

13 SafeGuard Configuration Protection

Con SafeGuard Configuration Protection è possibile definire le interfacce e i dispositivi periferici consentiti sui computer endpoint. Questo impedisce l'introduzione di malware e l'esportazione di dati tramite canali indesiderati quali, ad esempio, le WLAN. Questo modulo può inoltre di rilevare e bloccare hardware dannosi quali i key logger.

In generale, le porte o i dispositivi del computer possono essere abilitati o bloccati utilizzando criteri appropriati. L'utilizzo può essere inoltre limitato solo a determinati dispositivi.

È possibile impostare restrizioni per determinati dispositivi per le porte:

- USB
- PCMCIA

■ Firewire

Per queste porte è possibile definire i dispositivi da abilitare e quelli da bloccare.

Il responsabile della protezione definisce in modo centralizzato le porte e i dispositivi che è possibile utilizzare.

Se una determinata porta non è consentita, viene visualizzato un messaggio una volta ricevuto il relativo criterio. La porta non potrà essere utilizzata.

Il messaggio viene visualizzato come descrizione comando dell'icona di Configuration Protection sulla barra delle applicazioni di Windows.

Se nel computer sono state impostate restrizioni sull'utilizzo delle porte o dei supporti di archiviazione, il messaggio contenuto nella descrizione comando visualizza un avviso non appena si tenta di utilizzare porte o supporti di archiviazione non consentiti.

13.1 Procedura Challenge/Response per la sospensione del criterio di Configuration Protection

SafeGuard Configuration Protection può essere sospeso nei computer utilizzando la procedura di Challenge/Response.

Per far ciò, procedere secondo quanto riportato di seguito:

- Nei computer endpoint, è necessario richiedere una Challenge.
- Il responsabile dell'help desk crea il codice response che consente di sospendere il criterio nel computer per un determinato periodo di tempo.

13.2 Sospensione del criterio di Configuration Protection

Si deve essere in possesso del diritto di sospendere il criterio di Configuration Protection.

1. Nel computer, cliccare sull'icona dell'area di notifica e selezionare **Sospendi Configuration Protection**.
2. In **Sospendi Configuration Protection**, selezionare l'intervallo di tempo in cui si desidera eseguire la sospensione. Il codice challenge viene generato automaticamente. Resta valido per 30 minuti.
3. Contattare l'help desk via e-mail, SMS o telefono e fornire le informazioni richieste relative all'utente, al codice challenge e all'intervallo di tempo in cui si desidera venga eseguita la sospensione.
4. L'addetto all'help desk conferma le informazioni ricevute e fornisce all'utente il codice response tramite e-mail, SMS o telefono.
5. Nel computer, in **Sospendi Configuration Protection**, inserire o copiare il codice response fornito dall'help desk. Verificare che l'intervallo di tempo corrisponda a quello fornito dall'help desk. Cliccare su **OK**.

Il criterio di Configuration Protection viene quindi sospeso per l'intervallo di tempo specificato. Tale criterio può essere ripristinato in due modi:

- Durante l'intervallo di tempo della sospensione, nel computer, l'utente clicca sull'icona dell'area di notifica e seleziona **Ripristina Configuration Protection**.
- Una volta scaduto il tempo indicato per la sospensione, il criterio di Configuration Protection corrente viene ripristinato automaticamente.

13.3 Ripristino del criterio di Configuration Protection

Una volta scaduto l'intervallo di tempo indicato per la sospensione, il criterio corrente di Configuration Protection viene ripristinato automaticamente. Per ripristinare il criterio corrente di Configuration Protection manualmente, prima che l'intervallo di sospensione scada:

1. Nel computer, cliccare sull'icona dell'area di notifica e selezionare **Ripristina Configuration Protection**.
2. Cliccare su **Sì** per confermare.

Viene ripristinato il criterio corrente di Configuration Protection.

14 SafeGuard Enterprise e BitLocker Drive Encryption

La cifratura di unità BitLocker è una funzionalità completa di cifratura dei dischi con autenticazione in fase di preavvio inclusa nei sistemi operativi Windows Vista e Windows 7 di Microsoft. È progettata per proteggere i dati fornendo la cifratura per il volume di avvio.

14.1 Criteri di cifratura per BitLocker

Il responsabile della protezione può creare un criterio per la cifratura (iniziale) in SafeGuard Management Center e distribuirlo ai computer endpoint che utilizzano BitLocker, dove verrà eseguito.

Poiché i client BitLocker vengono gestiti in modo trasparente in SafeGuard Management Center, non è necessario che il responsabile della protezione configuri impostazioni BitLocker speciali per la cifratura. SafeGuard Enterprise è al corrente dello stato dei clienti e seleziona la cifratura BitLocker in modo conforme. Quando un client BitLocker è installato con SafeGuard Enterprise ed è attivata la cifratura del volume, tutti i volumi vengono cifrati da BitLocker.

14.2 Cifratura iniziale nel computer protetto da BitLocker

Quando il criterio di cifratura viene inviato al computer protetto da BitLocker, prima dell'avvio della cifratura iniziale nel computer, vengono generate da BitLocker le chiavi di cifratura. All'utente viene chiesto di specificare un percorso in cui installare la chiave di cifratura BitLocker. Inoltre, un backup di questa chiave viene memorizzato nel database di SafeGuard Enterprise per il recupero.

Quando SafeGuard Enterprise viene installato nel computer, l'icona del prodotto SafeGuard Enterprise viene visualizzata nell'area di notifica della barra delle applicazioni del computer. È possibile accedere in modo centralizzato a tutte le funzioni importanti fornite da SafeGuard

Enterprise nel computer. Le funzionalità disponibili variano in base alle impostazioni configurate nel SafeGuard Management Center. Tali impostazioni vengono configurate dal responsabile della protezione in modo centralizzato nel SafeGuard Management Center e distribuite ai computer endpoint.



Nota:

Se un disco rigido cifrato con BitLocker viene sostituito con un nuovo disco rigido e a quest'ultimo viene assegnata la stessa lettera dell'unità del disco precedente, viene salvata da SafeGuard Enterprise soltanto la chiave di recupero del nuovo disco rigido.

Se un volume è già stato cifrato con BitLocker prima dell'installazione del supporto BitLocker per SafeGuard Enterprise, è necessario eseguire il backup delle chiavi del volume cifrato in precedenza utilizzando le funzionalità di backup fornite da Microsoft.

14.3 Decifratura con BitLocker

I computer degli utenti cifrati con BitLocker non possono essere decifrati automaticamente. La decifratura deve essere eseguita utilizzando lo strumento "Manage-bde" Microsoft.

14.4 Autenticazione con BitLocker

BitLocker offre diverse opzioni di autenticazione. Gli utenti di BitLocker possono eseguire l'autenticazione tramite Trusted Platform Module (TPM) o stick USB, oppure una combinazione di entrambi.

In SafeGuard Management Center, il responsabile della protezione può impostare varie modalità di accesso in un criterio e distribuire tale criterio ai computer endpoint BitLocker.

Per gli utenti di SafeGuard Enterprise e BitLocker sono disponibili le seguenti modalità di accesso:

- Solo TPM
- TPM + PIN
- TPM + stick USB
- Solo stick (senza TPM)

Trusted Platform Module (TPM)

TPM è un chip simile a una smartcard, presente sulla scheda madre, che esegue funzioni di cifratura e operazioni di firma digitale. È in grado di creare, memorizzare e gestire chiavi utente ed è protetto dagli attacchi.

Stick USB

Le chiavi esterne possono essere memorizzate in uno stick USB non protetto.

Autenticazione sul computer BitLocker

Durante la fase di preavvio del computer BitLocker viene chiesto di inserire il PIN TPM o lo stick USB per l'autenticazione.

15 SafeGuard Enterprise e autocifratura, dischi rigidi conformi allo standard Opal

I dischi rigidi autocifrati offrono cifratura dei dati basata su hardware, quando tali dati sono scritti sul disco rigido. Il Trusted Computing Group (TCG) ha pubblicato lo standard indipendente Opal per dischi rigidi autocifranti. Diversi produttori offrono dischi rigidi conformi a Opal. SafeGuard Enterprise supporta lo standard Opal e offre la gestione dei computer endpoint con autocifratura, oltre che dischi rigidi conformi a Opal.

15.1 Cifratura dei dischi rigidi conformi a Opal

I dischi rigidi conformi a Opal sono autocifranti. I dati vengono cifrati automaticamente mentre vengono trascritti sul disco rigido.

I dischi rigidi conformi a Opal sono bloccati dalla chiave AES 256 utilizzata come password Opal. Questa password è gestita da SafeGuard Enterprise tramite un criterio di cifratura. Il responsabile della protezione definisce questo criterio di cifratura nel SafeGuard Management Center e lo distribuisce ai computer.

15.2 Icona dell'area di notifica ed estensioni di Esplora risorse su computer con dischi rigidi conformi a Opal

Quando SafeGuard Enterprise viene installato nel computer, l'icona del prodotto SafeGuard Enterprise viene visualizzata nell'area di notifica della barra delle applicazioni del computer. È possibile accedere in modo centralizzato a tutte le funzioni importanti fornite da SafeGuard Enterprise nel computer. Notare che le funzionalità disponibili variano in base alle impostazioni configurate nel SafeGuard Management Center. Tali impostazioni vengono configurate dal responsabile della protezione in modo centralizzato nel SafeGuard Management Center e distribuite ai computer endpoint.

Se il responsabile della protezione ha autorizzato l'utente, tramite relativo criterio, a decifrare dischi rigidi conformi a Opal, il comando **Decifra** di SafeGuard Enterprise sarà disponibile nel menu di scelta rapida di Esplora risorse.

16 SafeGuard Enterprise e Lenovo Rescue and Recovery

Per informazioni sulle versioni di Lenovo Rescue and Recovery (RnR) supportate da SafeGuard Enterprise, consultare il seguente articolo in inglese:

<http://www.sophos.com/support/knowledgebase/article/108383.html> .

È possibile ripristinare i backup completi dei sistemi operativi su una partizione cifrata senza dover prima decifrare il disco rigido. Ciò consente di risparmiare tempo durante un eventuale ripristino di emergenza. SafeGuard Enterprise è stato ufficialmente certificato da Lenovo per questa funzionalità.

La funzione principale di Lenovo Rescue and Recovery consiste nel ripristino dei dati, che è possibile eseguire semplicemente premendo un tasto. Anche se il sistema operativo principale è danneggiato e non può più essere avviato, Rescue and Recovery salva i dati tramite un ambiente di emergenza (WinPE). È possibile accedere agli strumenti di salvataggio da Microsoft Windows Desktop o premendo il tasto blu "ThinkVantage" integrato nei sistemi Lenovo.

Lenovo Rescue and Recovery è particolarmente utile per gli utenti mobili che non dispongono di supporto amministrativo. Risulta utile, ad esempio, in un viaggio di lavoro, per ripristinare il computer.

16.1 Panoramica

SafeGuard Enterprise è integrato nelle funzionalità Rescue and Recovery e supporta le funzionalità Lenovo come il tasto blu "ThinkVantage" sulla tastiera dei computer portatili Lenovo o il tasto blu "Enter" sulle tastiere dei PC.

Questa funzionalità integrata consente di combinare questo efficace metodo di backup e recupero con le partizioni cifrate del sistema operativo di SafeGuard Enterprise. I backup da sistemi cifrati SafeGuard Enterprise possono essere archiviati su qualsiasi unità disco utilizzata da RnR. Pertanto, in caso di emergenza, è possibile ripristinare un sistema caricando il backup da una partizione virtuale o di servizio o da un dispositivo rimovibile come un CD/DVD o un disco rigido USB.

Poiché il ripristino del sistema non influisce su SafeGuard Enterprise e tutte le impostazioni di cifratura rimangono inalterate, non è necessario reinstallare alcun software. Non è necessario riavviare la cifratura.

In un ambiente SafeGuard Enterprise, Rescue and Recovery è basato sul recupero di WinPE. WinPE può essere avviato da:

- una partizione virtuale o di servizio.
- un dispositivo rimovibile come un CD/DVD o un disco rigido USB.

16.2 Requisiti

- BIOS più recente per il PC/computer portatile.
- Per informazioni sulla compatibilità delle versioni di Rescue and Recovery con le versioni di SafeGuard Enterprise consultare il seguente articolo (in inglese):
<http://www.sophos.com/support/knowledgebase/article/108383.html>
- Lenovo Rescue and Recovery può essere utilizzato per recuperare i volumi cifrati di SafeGuard Enterprise. Deve essere installato il pacchetto di installazione SGNClient.msi.
- Per Rescue and Recovery i volumi devono essere cifrati con la chiave del computer definita. Per i volumi cifrati con altre chiavi, Rescue and Recovery non è supportato.

16.3 Installazione

Quando il software Rescue and Recovery è installato in un disco rigido senza una partizione di servizio, avviene quanto segue:

L'ambiente Rescue and Recovery è installato in una partizione virtuale all'interno della partizione "C:" del disco rigido (partizione principale del disco rigido master).

Nelle seguenti sezioni, notare la sequenza in cui vengono installati Rescue and Recovery e SafeGuard Enterprise. Si consiglia di installare prima Lenovo Rescue and Recovery, quindi SafeGuard Enterprise.

16.3.1 Installazione di Rescue and Recovery e SafeGuard Enterprise

Si consiglia la sequenza di installazione seguente:

1. Installare la versione più recente di Rescue and Recovery.
2. Installare la versione più recente del modulo SafeGuard Enterprise Device Encryption (**SGNClient.msi**).

SafeGuard Enterprise verifica che Rescue and Recovery sia installato e aggiunge i propri file e configurazioni all'ambiente di recupero di Lenovo.

3. Controllare che l'Autenticazione all'accensione sia attivata, in modo che non vengano ripristinati backup non autorizzati.

L'Autenticazione all'accensione viene attivata durante l'installazione di SafeGuard Enterprise.

16.3.2 Rescue and Recovery è già installato

RnR WinPE si trova sul primo disco rigido su una partizione di servizio o virtuale.

In questo caso tutti i driver e i file necessari vengono copiati nelle posizioni corrispondenti di RnR WinPE e le voci del Registro di sistema richieste vengono aggiunte ai file del registro di sistema di WinPE.

Installare la versione più recente del modulo SafeGuard Enterprise Device Encryption (**SGNClient.msi**).

SafeGuard Enterprise verifica che Rescue and Recovery sia installato e aggiunge i propri file e configurazioni all'ambiente di recupero di Lenovo (WinPE).

16.4 Upgrade

Un upgrade implica che siano installati SafeGuard Enterprise e Rescue and Recovery, e che si desideri aggiornare uno o entrambi ad una versione più recente.

Upgrade di SafeGuard Enterprise

Se si esegue l'upgrade di SafeGuard Enterprise, verrà aggiornato l'intero sistema, pertanto non sarà necessario impostare ulteriori configurazioni.

16.5 Disinstallazione

Quando si disinstallano i prodotti del software:

- Si consiglia di disinstallare prima SafeGuard Enterprise, quindi Rescue and Recovery. Se SafeGuard Enterprise viene disinstallato quando Rescue and Recovery è ancora installato, tutte le modifiche specifiche di SafeGuard Enterprise, ad esempio le unità, i file e le voci del registro di sistema aggiunti, vengono rimossi da RnR WinPE.
- Non disinstallare SafeGuard Enterprise subito dopo il ripristino del sistema. Dopo un ripristino del sistema, avviare il computer una volta, quindi disinstallare SafeGuard Enterprise.
- Se Rescue and Recovery viene rimosso mentre è ancora installato SafeGuard Enterprise, le modifiche di RnR del settore di avvio di MBR vengono rimosse e viene ripristinato il settore di avvio di MBR originale.

16.6 Ambiente di avvio e opzioni di recupero

SafeGuard Enterprise consente l'avvio nell'ambiente Rescue and Recovery dopo aver eseguito l'Accesso tramite autenticazione all'accensione (POA).

Dal disco rigido locale

- La partizione virtuale sul disco rigido locale o la partizione di servizio locale.
- I volumi devono essere cifrati in SafeGuard Enterprise con la chiave del computer definita. Tutti i driver necessari devono essere aggiunti a RnR WinPE. Quindi, la chiave del computer definita è disponibile nell'ambiente RnR WinPE e sarà possibile accedere nuovamente ai volumi.

Nota: SafeGuard Enterprise non consente di eseguire l'avvio nell'ambiente Rescue and Recovery quando si avvia direttamente da BIOS.

Da un CD/DVD di avvio o da un supporto rimovibile di avvio

- In questo caso non viene eseguita alcuna autenticazione durante POA, e non è disponibile alcuna chiave, pertanto non sarà possibile accedere ai volumi cifrati. Se si avvia Rescue and Recovery direttamente da BIOS, il sistema operativo verrà recuperato. SafeGuard Enterprise verrà rimosso durante il processo di ripristino. Per proteggere nuovamente il sistema, è necessario reinstallare SafeGuard Enterprise.

16.7 Creazione di un backup

I backup vengono creati in Windows mediante Rescue and Recovery. Su computer in cui è già installato Rescue and Recovery, e su cui SafeGuard Enterprise verrà installato in un secondo momento, viene visualizzato un messaggio che richiede all'utente di creare un nuovo backup del sistema.

Prima di creare un backup del sistema utilizzando Rescue and Recovery, leggere la documentazione fornita da Lenovo.

SafeGuard Enterprise fornisce assistenza solo per il salvataggio dei backup su:

- disco rigido locale
- secondo disco rigido
- disco rigido USB
- rete
- chiave USB
- CD/DVD

Per impostazione predefinita, i backup vengono salvati nella cartella C:\RRUbackups. Questa cartella è protetta da Rescue and Recovery se si trova su una partizione locale sull'unità disco rigido principale. In tal caso, non può essere eliminata o rimossa.

16.8 Ripristino dei backup dei file

Rescue and Recovery può ripristinare file o cartelle da backup in cui è installato SafeGuard Enterprise. Basta semplicemente avviare Windows, quindi Rescue and Recovery e ripristinare i file selezionati. Al termine del ripristino non è necessario riavviare il computer: è possibile lavorare sui file immediatamente.

16.9 Ripristino del sistema di SafeGuard Enterprise

Per ripristinare un backup di sistema che includa SafeGuard Enterprise, eseguire l'avvio nell'ambiente Rescue and Recovery. L'ambiente Rescue and Recovery viene visualizzato non appena si preme uno dei seguenti tasti durante il processo di avvio:

- "Thinkvantage" (computer portatili Lenovo)
- Tasto blu "Enter" (desktop-PC Lenovo)
- **F11** con le altre tastiere

1. Se si utilizza un computer Lenovo:

- a) Avviare l'ambiente Rescue and Recovery da un disco rigido locale premendo il tasto blu "ThinkVantage" sulla tastiera del computer portatile Lenovo o il tasto blu "Enter" sulla tastiera di un PC Lenovo.

Viene visualizzata la schermata dell'autenticazione all'accensione.

- b) Inserire le credenziali di SafeGuard Enterprise.

2. Se non si utilizza un computer Lenovo:
 - a) Accedere all'Autenticazione all'accensione con le proprie credenziali di SafeGuard Enterprise.
 - b) Mentre il computer procede con l'avvio, premere **F11** per avviare l'ambiente Rescue and Recovery.

Viene visualizzata l'interfaccia utente di Rescue and Recovery. Viene visualizzata la schermata iniziale.
3. Cliccare su **Avanti**.
4. Dal menu a sinistra scegliere **Ripristina backup**.

Viene visualizzata una finestra di dialogo in cui è possibile selezionare il backup.
5. Selezionare il backup e ripristinarlo.

16.10 Partizioni di servizio e partizioni di recupero predefinite

I nuovi computer Lenovo vengono forniti con partizioni speciali preinstallate:

- **Partizione di servizio Lenovo:** include l'ambiente di avvio Rescue and Recovery.
- **Partizione di recupero predefinita:** contiene tutte le informazioni sulle impostazioni e le funzioni di recupero predefinite del computer.

Queste partizioni sono visibili in Windows in unità diverse.

Nota: Quando queste partizioni sono disponibili sul computer, non verranno mai cifrate, neanche se è stato definito un criterio di cifratura per, ad esempio, la cifratura di tutti i volumi.

Se tali partizioni non sono presenti nel computer e si desidera crearne una, eseguire tale operazione prima di installare SafeGuard Enterprise. Per ulteriori informazioni, consultare la documentazione Lenovo.

16.11 Autenticazione all'accensione disabilitata e Lenovo Rescue and Recovery

Nel caso in cui l'Autenticazione all'accensione non sia attiva sul computer dell'utente, sarà necessario abilitare l'autenticazione Rescue and Recovery in modo tale da proteggere il computer dall'accesso a file crittografati dall'ambiente Rescue and Recovery.

Per informazioni dettagliate sull'attivazione dell'autenticazione Rescue and Recovery, consultare la documentazione di Lenovo Rescue and Recovery.

17 Supporto tecnico

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

- Visitando il forum SophosTalk su <http://community.sophos.com/> e cercando altri utenti con lo stesso problema.
- Visitando la knowledge base del supporto Sophos su: <http://www.sophos.it/support/>

- Scaricando la documentazione del prodotto su: <http://www.sophos.it/support/docs/>
- Inviando un'e-mail a support@sophos.com, indicando il o i numeri di versione del software Sophos in vostro possesso, i sistemi operativi e relativi livelli di patch, ed il testo di ogni messaggio di errore.

18 Note legali

Copyright © 1996 - 2011 Sophos Group. Tutti i diritti riservati. SafeGuard è un marchio registrato di Sophos Group.

Sophos è un marchio registrato di Sophos Limited, Sophos Group e Utimaco Safeware AG, qualora applicabile. Tutti gli altri nomi citati di società e prodotti sono marchi o marchi registrati dei rispettivi titolari.

Nessuna parte di questa pubblicazione può essere riprodotta, archiviata in un sistema di recupero, o trasmessa, in alcuna forma o in alcun mezzo, elettronico o meccanico, inclusi fotocopie, registrazioni e altri mezzi, salvo che da un licenziatario autorizzato a riprodurre la documentazione in conformità con i termini della licenza, oppure previa autorizzazione scritta del titolare dei diritti d'autore.

Informazioni relative al copyright di terzi sono reperibili nel file denominato "Disclaimer and Copyright for 3rd Party Software.rtf" nella directory del prodotto.