

SOPHOS

SafeGuard® Enterprise 5.50

Assistenza per l'utente

Data del documento: Agosto 2010



Sommario

| | | |
|----|--|-----|
| 1 | SafeGuard Enterprise sui PC utente | 2 |
| 2 | Autenticazione all'accensione..... | 4 |
| 3 | Autenticazione all'accensione con Windows Vista | 26 |
| 4 | Accesso a Windows Vista | 38 |
| 5 | Accesso mediante Lenovo Fingerprint Reader | 40 |
| 6 | Opzioni di recupero | 49 |
| 7 | Recupero via Local Self Help | 50 |
| 8 | Recupero mediante Challenge/Response..... | 60 |
| 9 | Icona dell'area di notifica e descrizione comandi..... | 71 |
| 10 | Estensioni SafeGuard Explorer | 74 |
| 11 | Crittografia dei dati..... | 77 |
| 12 | SafeGuard Data Exchange..... | 83 |
| 13 | SafeGuard Configuration Protection | 101 |
| 14 | SafeGuard Enterprise e BitLocker..... | 102 |
| 15 | SafeGuard Enterprise e Lenovo Rescue and Recovery..... | 104 |
| 16 | Supporto tecnico | 112 |
| 17 | Copyright | 113 |

1 SafeGuard Enterprise sui PC utente

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 un PC/notebook (client) sono la crittografia dei dati e la protezione dagli accessi non autorizzati a un computer mediante supporti esterni.

1.1 I 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.
- Crittografia basata su volume
- Supporto BitLocker

■ SafeGuard Data Exchange

- Scambio facile dei dati con supporti rimovibili su tutte le piattaforme, con ricrittografia dei dati.
- Crittografia basata su file
- Tutti i supporti rimovibili scrivibili, inclusi i dischi rigidi esterni e gli stick USB vengono crittografati in modo trasparente.

■ SafeGuard Configuration Protection

Utilizzando SafeGuard Configuration Protection è possibile consentire solo determinate interfacce o dispositivi periferici per i computer selezionati. Questo impedisce l'introduzione di 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: Le funzionalità disponibili sul proprio computer 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 mediante criteri e distribuite ai computer endpoint. Di conseguenza, è possibile che alcune funzionalità descritte in questo manuale non siano disponibili sul proprio computer.

2 Autenticazione all'accensione

Con l'Autenticazione all'accensione viene richiesto agli utenti di eseguire l'autenticazione durante la fase di preavvio del computer, ossia, prima dell'avvio del sistema operativo del computer. Dopo che l'utente è stato autenticato mediante l'Autenticazione all'accensione, viene avviato il sistema operativo (Windows) e l'utente accede automaticamente a Windows. La procedura è identica quando il computer esce da una fase di ibernazione (Suspend to Disk).



2.1 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 SafeGuard Enterprise esegue le modifiche necessarie tramite le impostazioni dei criteri nel SafeGuard Management Center.

Sono possibili le seguenti personalizzazioni:

- **Immagine di accesso**

La pagina di accesso predefinita visualizzata durante l'Autenticazione all'accensione è un design 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 della schermata dell'Autenticazione all'accensione sono visualizzati nella lingua predefinita, impostata nel computer mediante le Opzioni internazionali e della lingua di Windows al momento dell'installazione di SafeGuard Enterprise.

È possibile impostare la lingua predefinita in **Start > Impostazioni > Pannello di controllo > Opzioni internazionali e della lingua > Avanzate**. Se, ad esempio, questa impostazione è "Tedesco", il testo nella finestra di dialogo della POA verrà visualizzato in tedesco.

2.2 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 nel computer. 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 viene avviato il sistema operativo Windows.

Per l'accesso, SafeGuard Enterprise utilizza credenziali basate su certificato. 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. Soltanto gli utenti che hanno effettuato correttamente l'accesso a Windows su un sistema capace di comunicare con il server SGN possono essere autenticati mediante l'Autenticazione all'accensione.

Quando si effettua l'accesso per la prima volta dopo l'installazione, è necessario accedere a Windows come di consueto. Successivamente l'utente verrà registrato come utente SafeGuard Enterprise. Il processo di registrazione è necessario per assicurare che le credenziali dell'utente siano riconosciute 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 immesse le credenziali Windows dell'utente. L'accesso a Windows viene quindi eseguito automaticamente senza l'ulteriore immissione 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, vedere il file leggimi.

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

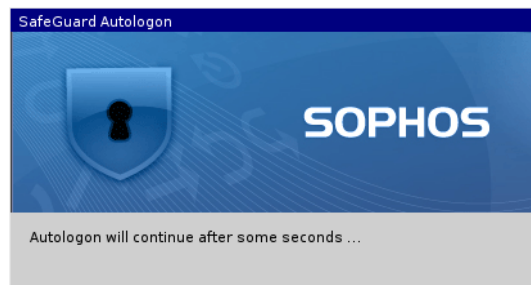
2.2.1 Prima procedura di accesso

La procedura del primo accesso corrisponderà a quella descritta, soltanto se l'Autenticazione all'accensione è stata installata e attivata sul computer.

A seconda della configurazione del sistema, è possibile che venga richiesto di premere **Ctrl+Alt+CANC** per continuare la procedura di accesso.

2.2.2 Accesso automatico SafeGuard

All'avvio del computer viene visualizzato l'Accesso automatico SafeGuard Enterprise.



Cosa succede?

1. Un utente ha effettuato l'accesso automatico.
2. Il computer viene automaticamente registrato sul server SafeGuard Enterprise, a condizione che sia attiva una connessione con il server SafeGuard Enterprise.
3. La chiave del computer viene inviata al server SafeGuard Enterprise e memorizzata nel database di SafeGuard Enterprise.
4. I criteri del computer vengono inviati al computer.

2.2.3 Accesso a Windows

Verrà visualizzata la finestra di dialogo di accesso a Windows.

Immettere le proprie credenziali Windows come di consueto.

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

Cosa succede?

1. Vengono inviati al server un ID utente e un hash delle credenziali utente.

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 che tutti i dati utente sopraccitati sono 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.

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

2.2.4 Autenticazione all'accensione dopo il riavvio del computer

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



Immettere 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.

L'opzione Passa attraverso l'accesso 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 immettere le proprie credenziali.

2.3 Accesso mediante l'Autenticazione all'accensione

Dopo l'attivazione dell'Autenticazione all'accensione, si effettua l'accesso immettendo le proprie credenziali utente di Windows nella finestra di dialogo di accesso dell'Autenticazione all'accensione. L'accesso a Windows verrà 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 **Passa attraverso l'accesso a Windows**.

Nota: 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](#), pagina 10).

2.3.1 Accesso posticipato nel caso di tentativo di accesso non riuscito

Se l'accesso all'Autenticazione all'accensione non riesce, ad esempio a seguito di un errore di digitazione della password, viene visualizzato un messaggio di errore e il tentativo di accesso successivo viene posticipato. L'intervallo di tempo di attesa viene aumentato ad ogni tentativo di accesso non riuscito. I tentativi non riusciti vengono registrati.

2.3.2 Blocco del computer

A seconda delle impostazioni dei criteri, dopo un certo numero di tentativi di accesso non riusciti, il computer può essere bloccato. Per sbloccare il computer, avviare una procedura Challenge/Response, vedere [Recupero mediante Challenge/Response](#), pagina 60.

2.3.3 Esempio di accesso utente mediante l'Autenticazione all'accensione

1. Utente 1 (Alice) accende il client XP.

Viene visualizzata la finestra di dialogo Accesso automatico dell'Autenticazione all'accensione.



2. Verrà quindi visualizzata la finestra di dialogo di accesso a Windows. Alice accede a Windows. Alice ora è il cosiddetto "proprietario". Esiste un solo proprietario per PC. Per impostazione predefinita, il primo utente a effettuare l'accesso è il proprietario.
3. Se i criteri utente, il certificato e la chiave si trovano tutti nel client, l'utente Alice viene creato all'interno del sistema SafeGuard Enterprise.
4. Dopo aver riavviato il computer, Alice può effettuare l'accesso durante l'Autenticazione all'accensione.



Nota: Se si applica l'impostazione predefinita, il primo utente ad accedere a Windows viene automaticamente registrato come "proprietario" del computer. A seconda del criterio, soltanto il proprietario di un computer può abilitare altri utenti ad accedere all'Autenticazione all'accensione. Nel nostro esempio solo Alice può accedere all'Autenticazione all'accensione.

Nota: Se altri utenti intendono accedere mediante l'Autenticazione all'accensione, dovranno chiedere l'autorizzazione al proprietario del computer (vedere [Importazione di altri utenti](#), pagina 10).

Nota: Il responsabile della protezione definisce nei relativi criteri, se attivare o meno l'opzione Passa attraverso l'accesso a Windows e se è consentito modificare questa impostazione nella finestra di dialogo di accesso.

2.4 Importazione di altri utenti

Un altro utente Windows (Bob) desidera accedere allo stesso computer al quale ha effettuato l'accesso Alice.

1. Bob accende il computer e viene visualizzata la finestra di dialogo dell'Autenticazione all'accensione.

Bob non può accedere mediante l'Autenticazione all'accensione, poiché non dispone delle chiavi e dei certificati necessari.

2. Perché Bob riesca ad accedere all'Autenticazione all'accensione, è necessario che il proprietario del computer (Alice) lo consenta.

Per impostazione predefinita, il primo utente a effettuare l'accesso dopo l'installazione viene registrato come il proprietario del computer.

Nota: Il responsabile della protezione può anche definire il proprietario di un computer tramite l'impostazione di un criterio.

3. Prima di eseguire l'accesso nell'Autenticazione all'accensione, Alice deve disattivare **Passa attraverso l'accesso a Windows**.



Viene visualizzata la finestra di dialogo di accesso a Windows, in cui viene richiesto a Bob di accedere.

4. Bob immette le sue credenziali Windows.

5. Se i criteri utente, il certificato e la chiave di Bob sono presenti nel computer (evidente dal relativo messaggio contenuto nel fumetto), l'utente Bob viene creato all'interno del sistema SafeGuard Enterprise.

Al successivo avvio del computer, Bob 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 il Management Center per assegnare gli utenti all'Autenticazione all'accensione su una nuova macchina. Dopo tale assegnazione, gli utenti potranno accedere a questi computer mediante l'Autenticazione all'accensione.

2.5 Password temporanea all'Autenticazione all'accensione

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

Esempio: il computer notebook viene avviato in un luogo pubblico, ad esempio all'aeroporto. Si pensa di essere stati osservati da qualcuno quando si immette la 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 durante l'Autenticazione all'accensione, in modo tale che nessun utente non autorizzato venga a conoscenza della password. Quando si è nuovamente connessi ad AD, verrà automaticamente richiesto di modificare la password temporanea.

Per modificare la password temporaneamente durante l'Autenticazione all'accensione:

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

Se non viene inserita la password in uso prima di premere **F8**, l'operazione verrà interpretata dal sistema come accesso errato e verrà visualizzato il relativo messaggio.

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

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

4. Fare clic su **OK**.

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

Verrà visualizzata la finestra di dialogo di accesso a Windows.

Nota: L'accesso non verrà eseguito tramite l'opzione Passa attraverso l'accesso a Windows, anche se il sistema è configurato in tal senso. Immettere qui la "vecchia password". La password temporanea è valida soltanto per l'accesso all'Autenticazione all'accensione.

5. Fare clic su **OK**.

L'utente è connesso a Windows.

Per l'accesso con l'Autenticazione all'accensione, ora è possibile utilizzare la password temporanea. La password temporanea è valida soltanto fino a quando essa non verrà modificata durante l'accesso a Windows. Soltanto dopo aver modificato la password temporanea sarà possibile accedere a Windows tramite l'Autenticazione all'accensione.

Modifica della password temporanea

La password modificata temporaneamente durante l'Autenticazione all'accensione deve essere modificata successivamente, al fine di sincronizzare nuovamente le password.

Quando si accede a Windows, in SafeGuard Enterprise viene chiesto automaticamente di modificare la password non appena si effettua nuovamente la connessione 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. Tuttavia può essere annullata ed è possibile utilizzare la "vecchia password" per l'accesso. La password potrà quindi essere modificata in un secondo momento.

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

Esistono due possibili tipi di accesso con smartcard o token:

- L'accesso è *consentito unicamente mediante smartcard o token.*
- L'accesso è consentito *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 protezione emette la smartcard/il token e lo fornisce all'utente, oppure è quest'ultimo a inserire le proprie credenziali Windows nella smartcard/nel token.

Nota: In SafeGuard Enterprise le smartcard e i token vengono gestiti allo stesso modo. Di conseguenza i termini "token" e "smartcard" possono essere intesi come la medesima cosa sia nel prodotto che nel manuale.

Nota: Nelle seguenti sezioni verrà utilizzato il termine "token".

2.6.1 Primo accesso con token dopo l'installazione

Il primo accesso effettuato con token è identico quello descritto nella procedura per l'accesso senza token.

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

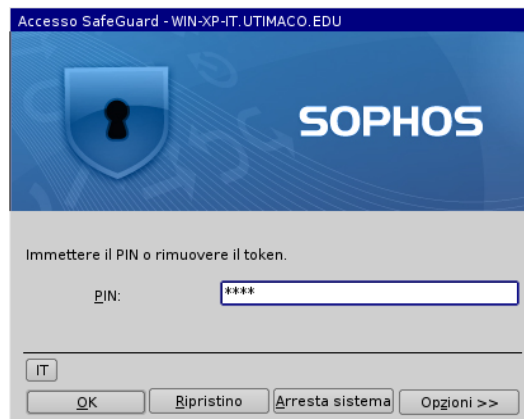
Nota: Si consiglia di configurare il token con le proprie credenziali Windows (vedere [Memorizzazione delle informazioni utente Windows nel token](#), pagina 16) prima di riavviare il computer. I criteri di protezione applicati all'utente potrebbero richiedere l'utilizzo di un token al momento dell'Autenticazione all'accensione. Se il token non contiene informazioni sull'utente, quest'ultimo non sarà in grado di accedere mediante l'Autenticazione all'accensione.

2.6.2 Accesso mediante l'Autenticazione all'accensione con token

assicurarsi che nel BIOS sia attivato il supporto USB. È necessario che sia stato inizializzato il supporto del token e che sia stato emesso un token per l'utente.

Come accedere mediante l'Autenticazione all'accensione utilizzando un token:

1. Inserire il token.
2. Accendere il computer e attendere che venga visualizzata la finestra di dialogo di accesso con token.



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

3. Immettere il PIN del token.

L'accesso viene effettuato mediante l'Autenticazione all'accensione e l'accesso a Windows (se l'opzione **Passa attraverso l'accesso a Windows** è attivata nella finestra di dialogo di accesso).

2.6.3 Modifica del PIN

È possibile modificare il PIN del token quando viene visualizzata la finestra di dialogo di accesso a Windows.

Se al momento dell'Autenticazione all'accensione (POA) è attivata l'opzione **Passa attraverso l'accesso a Windows**, la finestra di dialogo di accesso a Windows non viene in genere 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 (i criteri applicati potrebbero prevedere, ad esempio, la modifica del PIN a intervalli regolari).

Come modificare il PIN del token:

1. Nella finestra di dialogo PIN utilizzata per accedere a Windows, attivare **Modifica PIN**.



2. Immettere il PIN del token e fare clic su **OK**.

Viene visualizzata la finestra di dialogo Modifica PIN .



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

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

2.6.4 Memorizzazione delle informazioni utente Windows nel token

Se nel token non sono state memorizzate le informazioni utente, tali informazioni possono essere inserite nel token dall'utente stesso.

Nota: Si consiglia di configurare il token durante il primo accesso.

Nota: 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, quest'ultimo non sarà in grado di 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.
2. Se il sistema rileva un token vuoto, viene automaticamente visualizzata la finestra di dialogo per l'emissione di token.



3. Immettere nome utente e password di Windows.
4. Confermare la password.
5. Selezionare o immettere il dominio e fare clic su **OK**.

Viene effettuato il tentativo di accesso a Windows utilizzando i dati immessi. Se l'accesso riesce, i dati vengono scritti nel token.

L'utente è connesso a Windows.

Se l'accesso con token è definito come opzione facoltativa per l'utente (l'utente deve avere 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.

A tale scopo disattivare **Passa attraverso l'accesso a Windows (Opzioni > Passa attraverso l'accesso a Windows)** nella finestra di dialogo dell'Autenticazione all'accensione. Viene visualizzata la finestra di dialogo di accesso a Windows e sarà possibile memorizzare i dati nel token come descritto in precedenza.

2.6.5 Sblocco di smartcard o token

Se è stato immesso 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 per lo sblocco di un token bloccato:



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

Procedere nel modo seguente:

1. Immettere il PIN di amministratore.
2. Immettere un nuovo PIN e confermarlo.

Il PIN immesso 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. Fare clic su **OK**.

Il token viene sbloccato e la procedura di accesso viene continuata.

Nota: Se questa funzione non è disponibile nel computer, è possibile tornare ad accedere al computer tramite la procedura Challenge/Response.

Nota: Mediante la procedura Challenge/Response è possibile accedere nuovamente al computer. Tuttavia, non è possibile modificare il PIN o usare le credenziali utente tramite Challenge/Response.

2.6.6 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.

2.6.7 Token crittografici - Kerberos

Quando si utilizzano token crittografici, l'autenticazione all'accensione viene eseguita tramite un certificato memorizzato nel token.

Per questo tipo di accesso è necessario un token pienamente emesso per l'autenticazione. 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: Quando si utilizzano token di questo tipo, la procedura Challenge/Response non è disponibile nel caso di problemi di accesso. Se si verificano problemi di accesso, contattare il responsabile della protezione.

2.7 Accesso automatico dell'Autenticazione all'accensione con una smartcard o un token

assicurarsi che nel BIOS sia attivato il supporto USB. È necessario che sia stato inizializzato il supporto del token e che sia stato emesso un token per l'utente. Il rispettivo criterio è stato assegnato al computer.

Se al computer è stato assegnato un criterio corrispondente a un determinato PIN predefinito, tale criterio può consentire l'accesso automatico all'Autenticazione all'accensione mediante l'utilizzo di un token. All'accesso non sarà necessario immettere né le credenziali né il PIN, poiché questo avviene mediante l'Autenticazione all'accensione. Il passaggio attraverso Windows dipende dalle impostazioni dei criteri.

Come eseguire l'accesso automatico mediante 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. Il passaggio attraverso Windows dipende dalle impostazioni dei criteri.

- 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.

2.8 Tastiera virtuale

Durante l'Autenticazione all'accensione, l'utente può visualizzare/nascondere una tastiera virtuale e digitare i 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 del tipo **Impostazioni specifiche macchina applicabile**.

Per visualizzare la tastiera virtuale nell'Autenticazione all'accensione, fare clic su **Opzioni >>** nella finestra di dialogo dell'Autenticazione all'accensione e selezionare la casella di controllo **Tastiera virtuale**.



La tastiera virtuale supporta layout differenti ed è possibile, inoltre, modificare il layout mediante le stesse opzioni utilizzate per la modifica del layout di tastiera dell'Autenticazione all'accensione (vedere [Modifica del layout di tastiera](#), pagina 21).

2.9 Layout di tastiera

Quasi tutti i paesi hanno il proprio layout di tastiera, ossia, i tasti sono disposti diversamente. Il layout di tastiera nell'Autenticazione all'accensione è importante per l'immissione dei nomi utente, password e dei codici response.

Per impostazione predefinita, SafeGuard Enterprise adotta per l'Autenticazione all'accensione il layout di tastiera impostato nelle Opzioni internazionali e della lingua per l'utente predefinito di Windows al momento dell'installazione di SafeGuard Enterprise. Se in Windows il layout di tastiera è "Tedesco", tale layout verrà utilizzato anche nell'Autenticazione all'accensione.

La lingua utilizzata nel layout di tastiera 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).

2.9.1 Modifica del layout di tastiera

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

Per modificare la lingua del layout di tastiera:

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**, attivare **Applica tutte le impostazioni all'account utente corrente e al profilo utente predefinito**.
4. Fare clic su **OK**.

L'Autenticazione all'accensione riconosce il layout di tastiera utilizzato per l'ultimo accesso riuscito e lo riabilita automaticamente per il prossimo accesso. Questa operazione richiede il doppio riavvio del computer endpoint. Se il layout di tastiera precedente viene disattivato mediante **Opzioni internazionali e della lingua**, verrà tuttavia conservato fino a quando non venga selezionato uno differente.

Nota: Inoltre, per i programmi non Unicode è necessario modificare la lingua del layout di tastiera.

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, affinché l'Autenticazione all'accensione riesca a leggere il nuovo layout di tastiera, la seconda, affinché lo imposti.

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

È possibile visualizzare le lingue installate e disponibili per il sistema in uso mediante **Start > Esegui > regedit: HKEY_USERS\.DEFAULT\Keyboard Layout\Preload**.

2.10 Tasti di scelta/tasti funzione supportati nell'Autenticazione all'accensione

Alcune impostazioni e funzionalità hardware possono generare problemi durante l'avvio dei computer endpoint, 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 dell'Autenticazione all'accensione (POA, POA, Power-on Authentication) prima di eventuali distribuzioni importanti di SafeGuard Enterprise. Il file viene aggiornato mensilmente ed è disponibile per il download all'indirizzo: <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

È possibile personalizzare il file affinché rispecchi un particolare ambiente hardware.

Nota: Quando viene definito un file personalizzato, verrà utilizzato esclusivamente tale file anziché quello integrato nel file .msi. Nel caso in cui il file di configurazione dell'Autenticazione all'accensione non sia stato definito o trovato, verrà applicato il file predefinito.

Per installare il file di configurazione dell'Autenticazione all'accensione, immettere il comando seguente:

```
MSIEXEC /i <Client MSI package> POACFG=<path of the POA configuration file>
```

Per ulteriori informazioni, vedere la Knowledge Base:

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

Inoltre, l'Autenticazione all'accensione supporta molti tasti funzione.

2.10.1 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 **MAIUSC-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. |
| 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: Premendo **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**.

Nota: L'Autenticazione all'accensione può utilizzare la tastiera USB mediante BIOS SMM. Supporto token USB non disponibile.

2. Se il supporto USB non è disponibile, l'Autenticazione all'accensione tenta di utilizzare BIOS SMM invece di fare il back up e ripristinare il controller USB. In questa situazione, la modalità legacy può rappresentare una soluzione.

3. Supporto Legacy attivo, USB attivo. L'Autenticazione all'accensione tenta di eseguire il backup e ripristinare il 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 SafeGuard Enterprise mediante un file .mst .

Dopo aver modificato 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 **Sì**. Una volta riavviato il computer, le nuove impostazioni vengono attivate. Se si seleziona **No**, le modifiche non verranno salvate e la configurazione precedente rimarrà 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 verrà 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**.

2.10.2 I tasti funzione nella finestra di dialogo di accesso

Nota: I tasti funzione non sono tasti di scelta.

F2 = annullare Accesso automatico

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

F8 = modificare password dell'Autenticazione all'accensione. Utilizzare in alternativa al tasto **INVIO** per attivare la modifica della password in Autenticazione all'accensione dopo aver effettuato l'accesso.

Alt+MAIUSC (tasti a sinistra **Alt** e **MAIUSC**) = modificare lingua di tastiera da Tedesco a Inglese (o viceversa)

Annullamento e preparazione dell'Autenticazione all'accensione per arrestare il 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 è attivato l'accesso mediante impronte digitali, è possibile utilizzare **Ctrl+Alt+CANC** nella finestra di dialogo Autenticazione all'accensione, per accedere mediante impronte digitali e modificare la finestra di dialogo stessa affinché supporti l'accesso mediante nome utente e password. Per ulteriori informazioni sull'accesso con impronte digitali, vedere [Accesso mediante Lenovo Fingerprint Reader](#), pagina 40.

2.11 Sincronizzazione password

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

Se SafeGuard Enterprise rileva questo tipo di problema, viene richiesto all'utente di immettere la vecchia password. Una volta completata questa operazione, 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

L'Autenticazione all'accensione per Windows Vista ha lo stesso aspetto e funziona allo stesso modo rispetto a quella in uso per Windows XP (vedere [Autenticazione all'accensione](#), pagina 4). Le differenze riguardano soltanto la procedura di accesso al sistema operativo stesso. Windows Vista offre vari metodi di autenticazione per l'accesso degli utenti in parallelo.

Nota: In questa sezione vengono descritte soltanto le differenze relative a Windows Vista. Se non vengono esplicitamente evidenziate delle differenze, significa che le procedure e i processi descritti in precedenza si applicano anche a Vista.

3.1 Primo accesso dopo l'installazione di SafeGuard Enterprise in Windows Vista

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 nel computer. 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 verrà avviato il sistema operativo Windows.

Nota: In Windows Vista è necessario premere prima **Ctrl+Alt+CANC** per avviare l'accesso automatico e l'accesso. L'amministratore può disattivare questa impostazione nella console MMC dell'Editor oggetti Criteri di gruppo sotto Impostazioni di Windows > Impostazioni di protezione > Criteri locali > Disattiva opzioni di protezione (Accesso interattivo: **Ctrl+Alt+CANC** non richiesto).

Nota: SafeGuard Enterprise utilizza 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; ciò significa che solo dopo avere eseguito l'accesso a Windows è possibile effettuare l'autenticazione mediante l'Autenticazione all'accensione.

Pertanto, quando si effettua l'accesso per la prima volta dopo l'installazione, è necessario accedere a Windows correttamente utilizzando le proprie credenziali. In seguito l'utente viene registrato come utente SafeGuard Enterprise. Il processo di registrazione è necessario per assicurare che le credenziali dell'utente siano riconosciute 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 immesse le credenziali Windows dell'utente.

L'accesso a Windows viene quindi eseguito automaticamente senza l'ulteriore immissione di una password (se l'accesso automatico a Windows è attivato).

È possibile accedere mediante l'Autenticazione all'accensione immettendo il nome utente e la password.

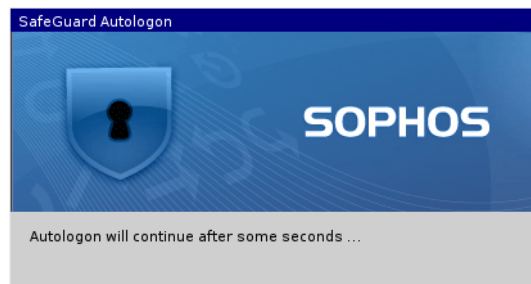
Nota: Le impostazioni per i PC utente nei quali è installato SafeGuard Enterprise sono definite in modo centralizzato dal responsabile della protezione nel SafeGuard Management Center e distribuite ai computer endpoint tramite file dei criteri.

3.1.1 Prima procedura di accesso

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

3.1.2 Accesso automatico SafeGuard

1. All'avvio del client viene visualizzato l'Accesso automatico SafeGuard Enterprise.



- Un utente ha effettuato l'accesso automatico.
- Il computer viene automaticamente registrato sul server SafeGuard Enterprise, a condizione che sia attiva una connessione con il server SafeGuard Enterprise.
- La chiave del computer viene inviata al server SafeGuard Enterprise e memorizzata nel database di SafeGuard Enterprise.
- I criteri del computer vengono inviati al computer.

3.1.3 Accesso a Windows Vista

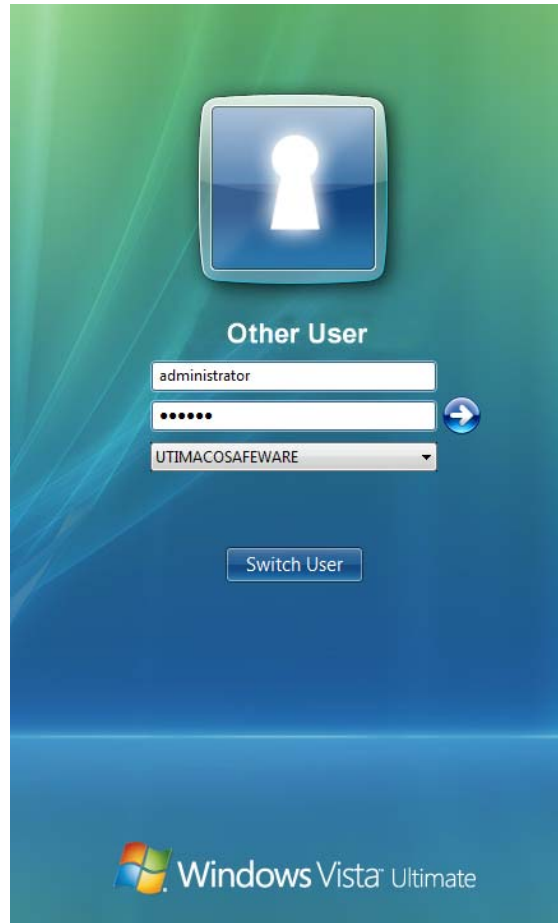
1. Viene visualizzata la finestra di dialogo di accesso a Windows Vista.



Con il sistema operativo Windows Vista, SafeGuard Enterprise offre un metodo di autenticazione aggiuntivo. L'esempio illustra il metodo di autenticazione SafeGuard Enterprise e le icone per il metodo di autenticazione Vista.

2. Windows Vista fornisce due icone per ciascun metodo di autenticazione:
 - Facendo clic su **Altro utente** si apre una finestra di dialogo per l'immissione delle credenziali.
 - Facendo clic sulla seconda icona (un nome utente è già visualizzato sotto l'icona) si apre una finestra di dialogo contenente le informazioni relative all'ultimo utente che ha effettuato l'accesso al sistema. È necessario immettere soltanto la password.

Se il proprio nome utente è visualizzato sotto un'icona SafeGuard Enterprise, selezionare l'icona appropriata. In caso contrario, selezionare l'icona SafeGuard Enterprise **Altro utente**.



3. Immettere le proprie credenziali Windows come di consueto.
 - Vengono inviati al server l'ID utente e un hash delle credenziali utente.
 - I criteri utente, i certificati e le chiavi vengono creati e inviati al client.

I dati utente sono disponibili nell'Autenticazione all'accensione soltanto dopo che tutti i dati sono stati sincronizzati tra il server 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 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.

3.1.4 Autenticazione all'accensione dopo il riavvio del computer

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



I certificati e le chiavi sono disponibili ed è possibile effettuare l'accesso mediante l'Autenticazione all'accensione utilizzando le proprie credenziali utente Windows.

2. Immettere il nome utente e la password e fare clic su **OK**.

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

Nota: L'opzione **Passa attraverso l'accesso 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 immettere le proprie credenziali.

3.2 Accesso mediante l'Autenticazione all'accensione in Windows Vista

Dopo l'attivazione dell'Autenticazione all'accensione (sincronizzazione iniziale e riavvio), si effettua l'accesso immettendo le proprie credenziali Windows nella finestra di dialogo di accesso dell'Autenticazione all'accensione. L'accesso a Windows verrà 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 **Passa attraverso l'accesso a Windows**. Ad esempio, è necessario disattivare l'accesso automatico per consentire ad altri utenti di utilizzare l'Autenticazione all'accesso sullo stesso computer. Il responsabile della protezione definisce, nei relativi criteri, se attivare o meno l'opzione Passa attraverso l'accesso a Windows e se è consentito modificare questa impostazione nella finestra di dialogo di accesso.

3.2.1 Accesso posticipato nel caso di tentativo di accesso non riuscito

Se l'accesso all'Autenticazione all'accensione non riesce, ad esempio a seguito di un errore di digitazione della password, viene visualizzato un messaggio di errore e il tentativo di accesso successivo viene posticipato. L'intervallo di tempo di attesa viene aumentato ad ogni tentativo di accesso non riuscito. I tentativi non riusciti vengono registrati.

3.2.2 Blocco del computer

A seconda delle impostazioni dei criteri, dopo un certo numero di tentativi di accesso non riusciti, il computer può essere bloccato. Per sbloccare il computer, avviare una procedura Challenge/Response, vedere [Recupero mediante Challenge/Response](#), pagina 60.

3.3 Accesso mediante l'Autenticazione all'accensione utilizzando smartcard o token in Windows Vista

Esistono due diversi tipi di accesso con smartcard o token:

- L'accesso è *consentito unicamente mediante smartcard o token.*
- L'accesso è consentito *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 protezione emette la smartcard/il token e lo fornisce all'utente, oppure è quest'ultimo a inserire le proprie credenziali Windows nella smartcard/nel token.

Nota: In SafeGuard Enterprise le smartcard e i token vengono gestiti allo stesso modo. Di conseguenza i termini "token" e "smartcard" possono essere intesi come la medesima cosa sia nel prodotto che nel manuale.

Nota: Nelle seguenti sezioni verrà utilizzato il termine token.

3.3.1 Primo accesso con token dopo l'installazione

Il primo accesso effettuato con token è identico quello descritto nella procedura per l'accesso senza token.

Se a questo punto 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 Windows (vedere vedere [Memorizzazione delle informazioni utente Windows nel token](#), pagina 35) prima di riavviare il computer.

Nota: 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, quest'ultimo non sarà in grado di accedere mediante l'Autenticazione all'accensione.

3.3.2 Accesso mediante l'Autenticazione all'accensione con token

Prerequisito: assicurarsi che nel BIOS sia attivato il supporto USB. È necessario che sia stato inizializzato il supporto del token e che sia stato emesso un token per l'utente.

Come accedere mediante l'Autenticazione all'accensione (POA) utilizzando un token:

1. Inserire il token.
2. Accendere il computer e attendere che venga visualizzata la finestra di dialogo di accesso con token.



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

3. Immettere il PIN del token.

L'accesso viene effettuato mediante l'Autenticazione all'accensione e l'accesso a Windows (se l'opzione "Passa attraverso l'accesso a Windows" è attivata nella finestra di dialogo di accesso).

3.3.3 Modifica del PIN

È possibile modificare il PIN del token quando viene visualizzata la finestra di dialogo di accesso a Windows.

Se al momento dell'Autenticazione all'accensione (POA) è attivata l'opzione **Passa attraverso l'accesso a Windows**, la finestra di dialogo di accesso a Windows non viene in genere visualizzata. Per aprire la finestra di dialogo di accesso a Windows, ad esempio, nel caso si desideri modificare il PIN, è necessario disattivare questa opzione durante l'accesso mediante l'Autenticazione all'accensione.

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

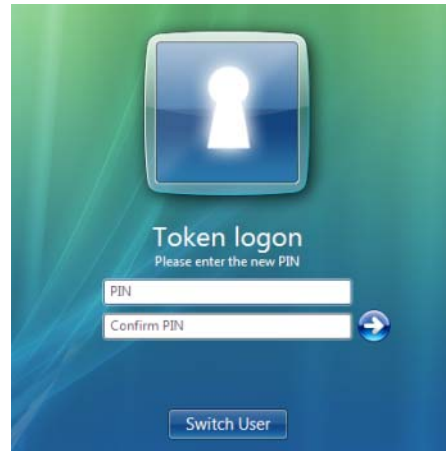
Come modificare il PIN del token:

1. Nella finestra di dialogo del PIN visualizzata per l'accesso a Windows, selezionare **Modifica PIN**.



2. Immettere il PIN del token e fare clic su **OK**.

Viene visualizzata la finestra di dialogo Modifica PIN .



3. Immettere il nuovo PIN e confermarlo.

4. Fare clic su **OK**.

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

3.3.4 Memorizzazione delle informazioni utente Windows nel token

Se nel token non sono state memorizzate le informazioni utente, tali informazioni possono essere inserite nel token dall'utente stesso.

Nota: Si consiglia di configurare il token al 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, quest'ultimo non sarà in grado di accedere mediante l'Autenticazione all'accensione.

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

Se il sistema rileva un token vuoto, viene automaticamente visualizzata la finestra di dialogo per l'emissione di token.



2. Immettere nome utente e password di Windows.
3. Confermare la password.
4. Selezionare o immettere il dominio e fare clic su **OK**.

Viene effettuato il tentativo di accesso a Windows utilizzando i dati immessi. Se l'accesso riesce, i dati vengono scritti nel token.

L'utente è connesso a Windows.

Se l'accesso con token è definito come opzione facoltativa per l'utente (l'utente deve avere 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.

A tale scopo, disattivare (**Opzioni > Passa attraverso l'accesso a Windows**) nella finestra di dialogo di accesso dell'Autenticazione all'accensione. Viene visualizzata la finestra di dialogo di accesso a Windows e sarà possibile memorizzare i dati nel token come descritto in precedenza.

3.3.5 Sblocco di smartcard o token con Windows Vista

Se viene immesso 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 per lo sblocco di un token:



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

Per sbloccare un token:

1. Immettere il PIN di amministratore.
2. Immettere un nuovo PIN e confermarlo.

Il PIN immesso 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. Fare clic su **OK**.

Il token viene sbloccato e la procedura di accesso viene continuata.

Se questa funzione non è disponibile nel computer, è possibile tornare ad accedere al computer tramite la procedura Challenge/Response.

Nota: Sebbene sia possibile recuperare l'accesso al computer mediante una procedura Challenge/Response, non è consentito modificare il proprio PIN, né le credenziali utente.

4 Accesso a Windows Vista

Con il sistema operativo Windows Vista, SafeGuard Enterprise offre un metodo di autenticazione aggiuntivo.

Se si disattiva l'opzione **Passa attraverso l'accesso a Windows** nella finestra di dialogo di accesso dell'Autenticazione all'accensione viene visualizzata la finestra di dialogo di accesso a Windows Vista. 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 è 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 mediante SafeGuard Enterprise

In genere l'accesso a Windows avviene automaticamente dopo aver immesso la password durante l'Autenticazione all'accensione. Se si disattiva l'opzione **Passa attraverso l'accesso 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 l'intera gamma delle funzionalità dopo aver effettuato l'accesso a Windows Vista.

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

4.2 Accesso tramite un metodo di autenticazione alternativo

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

Se si utilizza un metodo alternativo per accedere al sistema operativo, l'accesso a SafeGuard Enterprise viene eseguito dopo l'accesso al sistema operativo.

Dopo aver effettuato l'accesso a Windows Vista, l'applicazione per l'accesso SafeGuard Enterprise viene avviata automaticamente.

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'immissione del PIN.

1. Immettere le proprie credenziali o il PIN e fare clic su **OK**.

Ora la funzionalità SafeGuard Enterprise è disponibile e sarà possibile, ad esempio, accedere ai dati crittografati, a condizione che si disponga della chiave necessaria.

4.3 Sincronizzazione password con Windows Vista

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

Se SafeGuard Enterprise rileva questo tipo di problema, viene richiesto all'utente di immettere la vecchia password. Una volta completata questa operazione, 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.

5 Accesso mediante Lenovo Fingerprint Reader

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

Inoltre, non è possibile perdere o dimenticare le credenziali, né è possibile che persone non autorizzate possano eseguire l'accesso rubando i dati. Pertanto, l'utilizzo di lettori di impronte digitali semplifica la procedura di accesso migliorando la 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 sono integrati direttamente in determinati computer portatili Lenovo. Tuttavia, per l'accesso mediante impronte digitali, è possibile anche utilizzare una tastiera USB esterna.

- 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:

5.1.1 Requisiti generali

- Hardware Lenovo
- Lenovo Fingerprint Reader nel computer portatile o tastiera USB con lettore di impronte digitali.
- È consigliabile utilizzare il BIOS più recente
- SafeGuard Enterprise, versione 5.35 o successiva

- Prima di SafeGuard Enterprise, è necessario installare la versione software specifica del fornitore consigliato:
 - ThinkVantage Fingerprint per AuthenTecoppure
 - ThinkVantage Fingerprint per UPEK
- Il responsabile della protezione deve aver impostato l'opzione per le impronte digitali nel relativo criterio **Autenticazione**.

5.1.2 Requisiti di sistema

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

5.1.3 Hardware supportato

- AuthenTec AES2810
- UPEK TCS3C/TCD42A

5.1.4 Software supportato

- Lenovo Fingerprint per AuthenTec versione 3.2.0.166
- ThinkVantage Fingerprint per UPEK versione ' 3.2.0.166' #&

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 specifico del fornitore consigliato. La procedura di registrazione collega l'impronta registrata alle credenziali dell'utente (nome utente e password).

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

Per registrare le impronte digitali:

1. Eseguire l'accesso all'Autenticazione all'accensione (POA) immettendo nome utente e password.
2. Registrare una o più impronte digitali utilizzando il software specifico del fornitore installato. La procedura di registrazione collega l'impronta digitale alle credenziali di Windows.
 - a) Per informazioni su come registrare un'impronta digitale, vedere la documentazione del software ThinkVantage Fingerprint.
 - b) Abilitare l'opzione **POA password in BIOS** (solo per UPEK; per AuthenTec questo passaggio non è necessario).
 - c) Per utilizzare l'accesso mediante 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 l'impronta digitale registrata sul lettore. Per AuthenTec è, inoltre, necessario immettere la password di Windows al primo accesso.
3. Riavviare il PC/computer portatile.
4. Per provare 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 mediante 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 due impronte digitali.

1. Riavviare il PC/computer portatile.

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



2. Passare una delle dita registrate sul lettore.

Se l'impronta digitale viene riconosciuta, l'Autenticazione all'accensione legge le credenziali dell'utente e le invia a Windows.

Nota: La procedura di accesso utilizza icone con brevi messaggi di testo come prompt, notifiche e avvisi (vedere [Icone utilizzate durante la procedura di accesso](#), pagina 44).

L'accesso a Windows è stato eseguito automaticamente senza ulteriori richieste di dati.

- 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), in 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 il passaggio attraverso Windows. Le credenziali vengono trasferite al lettore di impronte digitali.

- Nei criteri applicabili all'utente il responsabile della protezione specifica se il passaggio attraverso 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](#), pagina 46).

5.3.1 Icone utilizzate durante la procedura di accesso

Quando si esegue l'accesso all'Autenticazione all'accensione con le impronte digitali, il sistema utilizza icone come prompt, notifiche e avvisi. Queste icone sono visualizzate durante la procedura di accesso insieme a un breve messaggio di testo.



Avvisa l'utente di passare il dito sul lettore di impronte digitali.



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.



Indica che il lettore di impronte digitali è in funzione e occupato.



Indica che l'impronta digitale è stata letta correttamente e che è stata trovata una corrispondenza.



Indica che l'impronta digitale è stata letta correttamente, ma che non è stata trovata alcuna corrispondenza.



Indica che non è possibile leggere l'impronta digitale. Passare nuovamente il dito sul lettore di impronte digitali.



Indica che il dito è stato posizionato troppo a sinistra (o troppo a destra). Spostare il dito al centro del lettore di impronte digitali.



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



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



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, viene effettuato un accesso posticipato.

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, viene effettuato un accesso posticipato.

Il periodo dell'accesso posticipato aumenta a 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.

Per eseguire l'autenticazione mediante l'immissione dei dati di accesso dell'utente:

1. Premere il tasto **Esc** oppure **Ctrl+Alt+CANC** nella finestra di dialogo dell'Autenticazione all'accensione mediante impronte digitali.

Viene visualizzata la finestra di dialogo per eseguire l'accesso mediante nome utente e password.



Nota: Se si seleziona **Ctrl+Alt+CANC** nella finestra di dialogo dell'Autenticazione all'accensione per l'accesso mediante nome utente e password, il computer viene arrestato. In questa finestra, la combinazione di tasti **Ctrl+Alt+CANC** equivale al pulsante **Arresta il sistema**.

La finestra di dialogo 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 (vedere [Avvio di una procedura Challenge/Response durante l'accesso mediante impronte digitali](#), pagina 48).

2. In alternativa, premere nuovamente **Esc** per tornare alla finestra di dialogo Autenticazione all'accensione per effettuare l'accesso mediante impronte digitali.

Se è stato premuto **Esc** per passare alla finestra di dialogo Autenticazione all'accensione per l'accesso mediante nome utente e password, è ancora possibile eseguire l'accesso passando il dito sul lettore senza dover prima tornare alla finestra di dialogo Autenticazione all'accensione per eseguire l'accesso mediante 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 **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, è possibile sincronizzare la password seguendo i passaggi riportati di seguito:

1. Riavviare il computer.
2. Premere il tasto **Esc** oppure **Ctrl+Alt+CANC** nella finestra di dialogo Autenticazione all'accensione, per accedere mediante impronte digitali e modificare la finestra di dialogo stessa affinché supporti l'accesso mediante nome utente e password.
3. Fare clic su **Opzioni** e disabilitare l'opzione **Passa attraverso l'accesso a Windows**.
Nei criteri applicabili all'utente il responsabile della protezione specifica se il passaggio attraverso 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.
4. Accedere con la password.
5. Verrà visualizzata la finestra di dialogo di accesso a Windows. Passare una delle dita registrate sul lettore.
6. L'impronta viene riconosciuta, ma la password collegata all'impronta digitale verrà rifiutata. Questa situazione non viene identificata come un tentativo di accesso non riuscito, tuttavia, non viene effettuato un accesso posticipato.
7. Viene visualizzato un messaggio che indica che la password è stata modificata e viene richiesto di immettere la password di Windows corrente. Immettere la password di Windows corretta.

Se viene immessa una password di Windows errata, viene registrato un tentativo di accesso non riuscito e viene effettuato un accesso posticipato. Se viene chiusa la richiesta di input senza immettere la password, viene registrato un tentativo di accesso non riuscito e viene effettuato un accesso posticipato

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

5.5 Avvio di una procedura Challenge/Response durante l'accesso mediante impronte digitali

Per il recupero dell'accesso è possibile eseguire una procedura Challenge/Response. Questo può essere necessario, ad esempio, se l'accesso mediante impronte digitali non funziona ed è stata dimenticata la password richiesta. La procedura Challenge/Response di SafeGuard Enterprise fornisce un metodo altamente protetto ed efficace per lo scambio di informazioni riservate.

Per avviare una procedura Challenge/Response con l'accesso mediante impronte digitali abilitato:

1. Premere il tasto **Esc** nella finestra di dialogo dell'accesso mediante impronte digitali.

Viene visualizzata la finestra di dialogo per eseguire l'accesso mediante nome utente e password.

2. fare clic sul pulsante **Recupero** per avviare la procedura Challenge/Response.

In seguito alla procedura Challenge/Response potrebbe essere consentito modificare la password durante l'avvio del computer, ad esempio, per abilitare il recupero in caso di password dimenticata. In questo caso, sarà possibile aggiornare le credenziali delle impronte digitali.

Per una descrizione dettagliata della procedura Challenge/Response, vedere [Recupero mediante Challenge/Response](#), pagina 60.

6 Opzioni di recupero

SafeGuard Enterprise offre varie opzioni di recupero (ad esempio, nel caso si sia dimenticata la password) adatte a scenari di recupero differenti:

■ Recupero dell'accesso via Local Self Help

Nel caso si sia dimenticata la password, l'utente può accedere al computer mediante Local Self Help senza richiedere l'assistenza all'help desk. Persino in assenza di connessione telefonica o ad una rete (ad esempio, a bordo di un aereo), 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 informazioni dettagliate, vedere [Recupero via Local Self Help](#), pagina 50.

■ Recupero mediante Challenge/Response

Il meccanismo Challenge/Response è un sistema di recupero sicuro ed efficace, che risulta molto utile all'utente nel caso non sia in grado di accedere al computer o ai dati crittografati. Durante la procedura Challenge/Response l'utente fornisce un codice challenge generato dal computer al responsabile dell'help desk, il quale, a sua volta, genera un codice response che autorizza l'utente a eseguire una determinata azione sul proprio computer.

Per informazioni dettagliate, vedere [Recupero mediante Challenge/Response](#), pagina 60.

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

7 Recupero via Local Self Help

Se la password è stata dimentica e non è possibile contattare l'help desk 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 inserendo un numero specificato o rispondendo a domande predefinite in Autenticazione all'accensione.

Il responsabile della protezione definisce in modo le domande a cui rispondere e le distribuisce ai computer endpoint. In alternativa, l'utente può creare le proprie domande, laddove il criterio applicato lo autorizzi a farlo. Per la creazione delle risposte iniziali e la modifica delle domande, SafeGuard Enterprise fornisce la procedura guidata di Local Self Help. Per aprire la procedura guidata di Local Self Help, fare clic sull'icona SafeGuard Enterprise dell'area di notifica nella barra delle applicazioni di Windows.

7.1 Prerequisiti

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

- Il responsabile della protezione ha abilitato Local Self Help nel criterio valido e applicato appartenente al tipo **Impostazioni generali** e ha stabilito le impostazioni relative a questa funzione (ad esempio, l'autorizzazione a creare le domande personalmente).
- Local Self Help è attivato sul computer dell'utente (vedere [Attivazione di Local Self Help](#), pagina 51).

7.2 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 diviene attivo sul computer dell'utente solo dopo che questo abbia risposto e salvato almeno dieci domande. A seconda delle impostazioni dei criteri si possono generare le seguenti situazioni:

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

Rispondere e salvare almeno dieci delle domande predefinite ricevute.

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

Rispondere e salvare almeno dieci domande (le domande predefinite, le domande create 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 almeno dieci domande.

Nota: Per accedere all'Autenticazione all'accensione via Local Self Help, è necessario rispondere a cinque domande selezionate casualmente fra le dieci domande con risposta.

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. Fare clic sull'icona SafeGuard Enterprise dell'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 immettere la password.

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

Viene visualizzata la finestra di dialogo Panoramica sullo stato .

Questa finestra di dialogo fornisce brevi informazioni su come attivare Local Self Help. Inoltre, consente di visualizzare informazioni sullo stato (ad esempio, il numero di domande definite dall'utente a cui è stata data una risposta, il numero di domande predefinite con una risposta, ecc.).

4. Fare clic su **Avanti**.

Una volta ricevute le domande predefinite assieme al criterio valido, viene visualizzata la finestra di dialogo Domande predefinite .

| Domande | Risposte | Tema |
|---|------------------------------|----------|
| In quale città o paese vorresti vivere? | <fare clic qui per rispon... | Italiano |
| Chi è il tuo sportivo preferito? | <fare clic qui per rispon... | Italiano |
| Qual è il tuo piatto preferito? | <fare clic qui per rispon... | Italiano |
| Chi era il tuo idolo quando eri ragazzo? | <fare clic qui per rispon... | Italiano |
| Qual era il nome del tuo primo animale domestico? | <fare clic qui per rispon... | Italiano |
| Che cosa ti spaventava di più da piccolo? | <fare clic qui per rispon... | Italiano |
| Qual era la tua prima automobile? | <fare clic qui per rispon... | Italiano |
| Qual è il tuo film preferito? | <fare clic qui per rispon... | Italiano |
| Chi è il tuo attore/attrice preferito? | <fare clic qui per rispon... | Italiano |
| Qual è il cognome da nubile di tua madre? | <fare clic qui per rispon... | Italiano |
| Chi è il tuo artista preferito? | <fare clic qui per rispon... | Italiano |
| In che anno è nato tuo padre? | <fare clic qui per rispon... | Italiano |

Per l'attivazione, immettere altre 10 risposte.

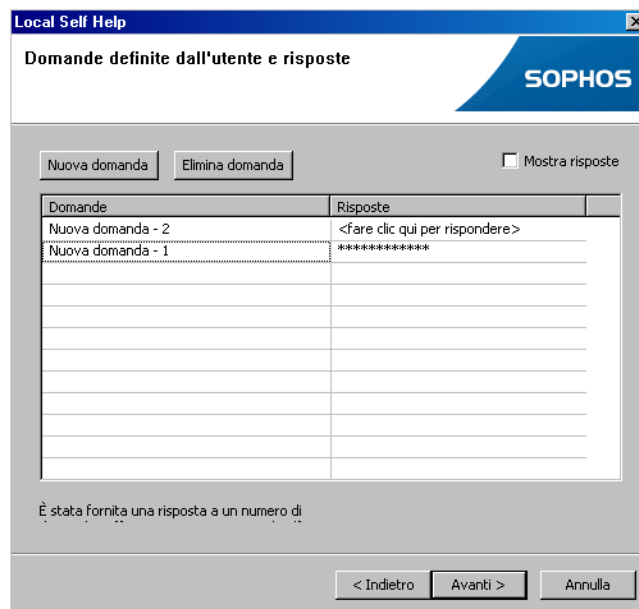
< Indietro Avanti > Annulla

- Se l'utente ha ricevuto domande relative a vari argomenti, può scegliere 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, selezionare la domanda e inserire la risposta nella colonna **Risposte**.
- Una volta immessa 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 di Local Self Help. In Local Self Help, per le risposte viene fatta distinzione fra maiuscole e minuscole.

Nota: Quando si inseriscono le risposte in Giapponese, è necessario utilizzare i caratteri romani. Altrimenti, le risposte non verranno decodificate correttamente al momento del loro inserimento nell'Autenticazione all'accensione.

5. Una volta risposto alle domande predefinite, fare clic su **Avanti**.
6. Se l'utente è autorizzato a creare le domande personalmente, viene visualizzata la finestra di dialogo Domande e risposte definite dall'utente .



- a) Per aggiungere una nuova domanda, fare clic 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 di Local Self Help. In Local Self Help, per le risposte viene fatta distinzione fra maiuscole e minuscole.

Nota: Quando si inseriscono le risposte in Giapponese, è necessario utilizzare i caratteri romani. Altrimenti, le risposte non verranno decodificate correttamente al momento del loro inserimento nell'Autenticazione all'accensione.

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

L'ultima finestra di dialogo visualizzata nella procedura guidata Local Self Help consente di controllare le informazioni sul nuovo stato, una volta risposto alle domande. Un messaggio indica se i prerequisiti per l'attivazione di Local Self Help sono stati soddisfatti o meno.

8. Fare clic su **Fine**.

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

9. Fare clic 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 necessario reimpostare la password mediante una procedura Challenge/Response, le risposte memorizzate in Local Self Help non saranno più valide. Local Self Help non è più attivo sul computer dell'utente. Per riattivare Local Self Help, rispondere nuovamente alle domande.

7.3 Modifica delle domande

Dopo l'attivazione di Local Self Help sul computer dell'utente, 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.

Per modificare le domande durante la procedura guidata Local Self Help:

1. Fare clic sull'icona SafeGuard Enterprise dell'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 immettere la password.

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

Viene visualizzata la finestra di dialogo di Panoramica sullo stato .

Questa finestra di dialogo fornisce brevi informazioni su come attivare Local Self Help. Inoltre, consente di visualizzare informazioni sullo stato (ad esempio, il numero di domande definite dall'utente a cui è stata data una risposta, il numero di domande predefinite con una risposta, ecc.).

4. Fare clic su **Avanti**.

- a) Nel caso in cui l'utente abbia ricevuto e risposto alle domande predefinite, viene visualizzata la finestra di dialogo delle domande predefinite, in cui vengono indicate le risposte.
- b) Se l'utente ha ricevuto domande relative a vari argomenti, può scegliere 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 immesso, attivare la casella di controllo **Mostra risposte**.
- e) Per modificare le risposte, fare clic sulle relative domande e inserire la nuova risposta nella colonna **Risposte**.

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

Se l'utente è autorizzato a creare le domande personalmente, viene visualizzata la finestra di dialogo Domande e risposte definite dall'utente. Per impostazione predefinita, le risposte inserite non vengono visualizzate come testo.

6. Per visualizzare il testo inserito, fare clic sulla casella di controllo **Mostra risposte**.

- a) Per modificare le risposte esistenti, fare clic sulle relative domande e inserire la nuova risposta nella colonna **Risposte**.
- b) Per aggiungere una nuova domanda, fare clic 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, fare clic sulla domanda in questione e selezionare il pulsante **Elimina domanda**.

Viene visualizzato un messaggio che richiede all'utente se desidera eliminare la domanda. Fare clic su **Sì**.

7. Per completare l'operazione di modifica, fare clic su **Avanti**.

L'ultima finestra di dialogo visualizzata nella procedura guidata Local Self Help consente di controllare le informazioni sul nuovo stato, una volta modificate le domande. Un messaggio indica se i prerequisiti necessari perché Local Self Help rimanga attivo sono stati soddisfatti o meno.

8. Fare clic su **Fine**.

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

9. Fare clic su **OK**.

Le modifiche apportate sono attive

Al prossimo 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: Se il numero di domande con risposta fosse inferiore al numero minimo richiesto a causa delle modifiche apportate, viene visualizzato un messaggio di errore nell'ultima finestra di dialogo della procedura guidata Local Self Help che informa l'utente che al termine della procedura guidata Local Self Help verrà disattivato.

Nota: Se non si desidera disattivarlo, è possibile tornare alle finestre di dialogo **Domande definite dall'utente** e **Domande predefinite**, facendo clic sul pulsante **Indietro**. Quindi sarà 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 errore, che informa che Local Self Help non sarà più attivo sul computer dell'utente. Tuttavia, è possibile riattivare Local Self Help (vedere [Attivazione di Local Self Help](#), pagina 51).

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

Per accedere all'Autenticazione all'accensione via Local Self Help, è necessario rispondere correttamente a cinque domande selezionate casualmente fra le dieci domande definite.

Come accedere al computer mediante Local Self Help nell'Autenticazione all'Accensione:

1. Immettere il nome utente nella finestra di dialogo dell'Autenticazione all'accensione.

Il pulsante **Recupero** diviene attivo.

2. Fare clic su **Recupero**.

- Se viene attivato solo Local Self Help per il recupero dell'accesso, allora viene avviato.
- 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. Fare clic su **Local Self Help**.

Viene visualizzata la finestra di dialogo di benvenuto di Local Self Help .

Questa finestra fornisce una breve descrizione dei passaggi che seguiranno.

3. Fare clic su **Avanti** per iniziare a rispondere alle domande.

La prima domanda viene visualizzata nella finestra di dialogo Local Self Help - Domanda 1 di 5 .

4. Immettere la risposta.

Per impostazione predefinita, il testo inserito non viene visualizzato nel campo di immissione per motivi di sicurezza. Per visualizzare la risposta, deselezionare la casella di controllo **Nascondi risposta**.



5. Dopo aver risposto alla domanda, fare clic su **Avanti**.

Una volta risposto a una domanda, è possibile fare clic su **Avanti** e procedere con quella successiva.

6. Rispondere alle restanti quattro domande. Dopo aver risposto all'ultima, fare clic su **OK**.

Nella finestra di dialogo successiva è possibile visualizzare la password corrente.

7. Per visualizzare la password, premere nuovamente **INVIO** o la **BARRA SPAZIATRICE** oppure chiudere la casella blu.

NON fare clic su **OK**. **Dopo aver fatto clic 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 password premendo **BARRA SPAZIATRICE**, **INVIO** oppure facendo clic sulla casella di visualizzazione blu.

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

Ora si dispone dell'accesso all'Autenticazione all'accensione e a Windows.

7.5 Tentativi di accesso non riusciti

Se per una o più domande si immette una risposta errata, non sarà possibile accedere. In tal caso viene visualizzato un messaggio che indica che l'accesso non è riuscito. Per ragioni di sicurezza, Local Self Help non segnala quale delle risposte fornite non era corretta.

Una procedura di recupero di Local Self Help non riuscito è considerata come un tentativo di accesso non riuscito e registrata come evento. In tal caso, viene effettuato un accesso posticipato. Il periodo dell'accesso posticipato aumenta a ogni tentativo di accesso non riuscito.

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

7.6 Riattivare le domande e le risposte dopo aver modificato la password di diversi computer

Se Local Self Help è attivato per l'utilizzo su computer differenti e viene modificata la password di Windows su un computer, una volta che tale modifica sia divenuta effettiva, le domande e le risposte memorizzate in Local Self Help non saranno più valide sulla seconda ed eventuali altre macchine. Tuttavia, 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.

Procedere nel modo seguente:

1. Una volta la modificata la password sul computer in questione, accedere alla seconda macchina.

Una notifica informa l'utente che sono presenti delle domande di Local Self Help cui non è stato risposto.

2. Fare clic sull'icona SafeGuard Enterprise 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. Immettere la password e fare clic su **Avanti**.
4. Confermare tutte le pagine della procedura guidata Local Self Help, selezionando **Avanti** e facendo clic su **Fine** nell'ultima pagina.

Le domande e le risposte archiviate 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 Challenge/Response

Per il recupero SafeGuard Enterprise offre una **procedura Challenge/Response** per lo scambio di informazioni riservate. La procedura Challenge/Response è sicura e efficace.

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 in primo luogo Local Self Help per recuperare una password dimenticata. Il recupero tramite Local Self Help consente di visualizzare la password attuale in maniera riservata nell'Autenticazione all'accensione e sarà possibile continuare utilizzando tale password. Ciò consente di evitare la reimpostazione completa della password ed eventuali richieste di assistenza all'help desk.

Durante la procedura Challenge/Response l'utente genera un codice challenge (una stringa di caratteri ASCII) e fornisce tale codice a un membro del personale dell'help desk. In base al codice challenge fornito, il responsabile dell'help desk genera a sua volta un codice response che autorizza l'utente a eseguire una determinata azione sul proprio computer.

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

- L'utente ha dimenticato la password.
- L'utente ha immesso troppe volte una password non corretta a livello di Autenticazione all'accensione e 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 client **SafeGuard 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 consentirà di accedere al computer senza reimpostare la password.

Se una password incorretta è stata immessa troppe volte, l'help desk genererà automaticamente un codice response per consentire l'avvio del client senza l'accesso utente (lo scenario è incluso 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, richiedere una challenge senza tentare di immettere prima la password. L'help desk potrà quindi generare un codice response per l'accesso con e senza un nome utente. Quando si effettua l'accesso con il proprio nome utente, richiedere all'help desk di visualizzare la vecchia password durante la procedura Challenge/Response. Ciò consente di evitare la reimpostazione della password. Al contrario, 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](#), pagina 67).

- Ripristino della cache dei criteri **SafeGuard Enterprise**:

Questa procedura è necessaria se la cache dei criteri è danneggiata. Nella cache locale sono memorizzate le chiavi, i criteri, i certificati dell'utente e i file di controllo. 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 Challenge/Response, 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 Challenge/Response.

- **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. A tale scopo, selezionare **Continua l'avvio da: disco floppy/supporto esterno** nella finestra di dialogo di accesso mediante l'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 La procedura Challenge/Response

1. Viene avviata l'Autenticazione all'accensione (POA).

Dal momento in cui viene generata la challenge è disponibile un intervallo di 30 minuti per immettere correttamente il codice response generato dall'help desk in una procedura Challenge/Response. Dopo 30 minuti il codice response 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. Immettere 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 fare clic su **Recupero**.

Il pulsante **Recupero** viene attivato soltanto quando si immette 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.

Challenge/Response - passaggio 2 di 3

SOPHOS

Se si è dimenticata la password, è possibile chiamare l'Helpdesk e richiedere una password per l'uso singolo.

Dominio utente: MY_COMPANY

ID utente:

Dominio computer: MY_COMPANY.EDU

ID computer: WIN-XP-IT

Challenge: ISDN2 GAG5S 3AJN3 AGJKG WS7M9 65925

Questa challenge scadrà tra: 14:56 minuti

Indietro Avanti Annulla Aiuto ortogr.

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

Per facilitare il processo di comunicazione del codice challenge, è possibile visualizzare un aiuto ortografico selezionando il pulsante **Aiuto ortografico**.

Il responsabile dell'help desk sarà in grado di identificare dal codice challenge lo scenario per il quale è necessario fornire un codice response.

3. Fare clic su **Avanti**.

8.5 Inserimento del codice response

1. Immettere il codice response ricevuto dal responsabile dell'help desk nella finestra di dialogo Response e confermare facendo clic su **OK**.

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

2. L'utente verrà connesso al momento dell'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 incorretta

1. È stata immessa troppe volte una password incorretta durante l'Autenticazione all'accensione (errori di digitazione, tasto **BLOC MAIUSC** attivato e così via), tuttavia si è a conoscenza della password corretta. L'utente è connesso al dominio.
2. Il PC è bloccato e viene chiesto di iniziare una procedura Challenge/Response per sbloccare il computer.
3. Il responsabile dell'help desk genera un codice response per l'avvio senza l'accesso utente.
4. L'avvio senza l'accesso significa che non è necessario modificare la password prima di accedere a Windows. Viene visualizzata la finestra di dialogo di accesso a Windows. È possibile immettere la propria password Windows in questa finestra di dialogo per accedere al sistema.
5. Il contatore del numero massimo di tentativi di immissione della password viene reimpostato.

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 utilizzare in primo luogo i metodi seguenti per recuperare una password dimenticata, per evitarne la reimpostazione in modo centralizzato:

- Utilizzare Local Self Help. Il recupero tramite Local Self Help consente di visualizzare la password attuale e di continuare utilizzando tale password senza doverla reimpostare e senza richiedere assistenza all'help desk. Per ulteriori informazioni, vedere [Recupero via Local Self Help](#), pagina 50.
- Quando si utilizza Challenge/Response: Richiedere all'help desk di generare un codice response con accesso utente e di visualizzare la vecchia password durante la procedura Challenge/Response. Ciò consente di evitarne la reimpostazione. È possibile continuare a utilizzare la vecchia password e modificarla localmente in un secondo momento, se necessario.

Se non è possibile applicare i due metodi descritti in precedenza, procedere come segue:

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 L'utente ha dimenticato o ha perso il token.

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

1. Viene richiesto di modificare la password durante la procedura Challenge/Response. 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, facendo clic su **Annulla**.

- **L'utente ha dimenticato il token**

Saltare la modifica della password facendo clic su **Annulla** nella finestra di dialogo ha senso soltanto se si è dimenticato il token e sarà comunque possibile utilizzarlo per effettuare l'accesso in futuro. Se si fa clic 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 dimenticato il token**

Se il token è stato dimenticato, immettere una nuova password nella finestra di dialogo per la modifica della password. Con questa password verrà 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 mediante l'Autenticazione all'accensione utilizzando questa password.

L'utilizzo non autorizzato del token da parte di qualsiasi utente che ne entra in possesso per caso è escluso. 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 ha dimenticato il PIN del token, l'utente deve richiedere un codice response e immettere una nuova password. Con questa password viene effettuato l'accesso a Windows ed è possibile utilizzarla anche per accedere mediante l'Autenticazione all'accensione, a condizione che l'utente sia autorizzato all'accesso mediante l'utilizzo di una password.
2. Un responsabile della protezione deve assegnare al token un nuovo PIN e memorizzarvi i nuovi dati di accesso. In seguito sarà possibile utilizzarlo nuovamente per l'accesso.

8.6.5 Non è più possibile accedere al computer

Se non è più possibile accedere al computer, è possibile che l'Autenticazione all'accensione sia danneggiata. Persino in questa situazione critica SafeGuard Management Center offre una procedura Challenge/Response con assistenza all'help desk che consente di recuperare l'accesso ai propri dati crittografati. In questo caso la procedura Challenge/Response viene eseguita mediante un ambiente WinPE. In una situazione di questo tipo, si consiglia di contattare il proprio help desk SafeGuard Management Center. Il responsabile dell'help desk fornisce all'utente i file necessari e lo guida 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) 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 la password è stata dimenticata. La procedura Challenge/Response consente di 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, sarebbe necessario 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. Si consiglia di 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 segue:

1. Iniziare la procedura Challenge/Response facendo clic 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. Fare clic su **Avanti** nella finestra di dialogo Challenge/Response e immettere il codice response.

5. Fare clic su **OK**.
6. Verrà chiesto se la vecchia password deve essere visualizzata sullo schermo.



7. Scegliere **SÌ** e fare clic su **OK**.
8. La finestra di dialogo successiva informa che la password verrà visualizzata premendo **INVIO** o la **BARRA SPAZIATRICE** oppure facendo clic sul testo.

NON fare clic su **OK**. Dopo aver fatto clic su **OK** il processo di avvio continuerà infatti **SENZA** che la password venga visualizzata.

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

9. Premere **INVIO** o la **BARRA SPAZIATRICE** oppure fare clic sul testo.

Verrà visualizzata la password.

Nota: Prendere tutte le dovute precauzioni affinché nessun utente non autorizzato possa vedere, involontariamente o volontariamente, il contenuto della schermata. È possibile nascondere immediatamente la password premendo **BARRA SPAZIATRICE**, **INVIO** o facendo clic con il mouse. La password verrà mostrata per un intervallo di tempo massimo di 5 secondi.



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

Sarà 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 in base al fatto se si è a conoscenza o meno delle proprie credenziali Windows.

- Si è a conoscenza delle proprie credenziali Windows

- a) Se le credenziali Windows sono conosciute, iniziare la procedura Challenge/Response come descritto. Si accede automaticamente a Windows e si può utilizzare il computer.

- La modalità di accesso "solo token" viene reimpostata per la durata della sessione di lavoro durante la 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 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 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 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).

- **Local Self Help**

Se Local Self Help è attivato per il computer in uso mediante il criterio relativo, 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'help desk. Per ulteriori informazioni su Local Self Help, vedere [Recupero via Local Self Help](#), pagina 50.

- **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](#), pagina 83).
- **Sincronizza:** Avvia la sincronizzazione dei dati con il server SafeGuard Enterprise. 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 |
|---|--|
| Ultima ricezione di un criterio | Mostra la data e l'ora di ricezione dell'ultimo criterio. |
| Ultima ricezione di una chiave | Mostra la data e l'ora di ricezione dell'ultima chiave. |
| Ultima ricezione di un certificato | Mostra la data e l'ora di ricezione dell'ultimo certificato. |
| Ultimo contatto con il 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"> ■ In sospeso 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. ■ Utente SGN L'utente è stato assegnato all'installazione di SafeGuard Enterprise come utente SafeGuard Enterprise. ■ Guest SGN 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. ■ Guest SGN (account di servizio) 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. ■ Sconosciuto Indica che non è possibile determinare lo stato dell'utente. |
| Stato della cache locale Pacchetti di dati preparati per la trasmissione | Indica se sono presenti pacchetti da inviare al server SafeGuard Enterprise. |

| Campo | Informazioni |
|---|---|
| Stato Local Self Help (LSH) Abilitato Attivo | Indica se Local Self Help è stato abilitato mediante criteri e se è stato attivato sul computer dall'utente. Per ulteriori informazioni su Local Self Help, vedere Recupero via Local Self Help , pagina 50 |

- **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 Estensioni SafeGuard Explorer

È possibile accedere alle funzioni per la crittografia tramite le rispettive voci dei menu di scelta rapida in Esplora risorse.

10.1 Estensioni Explorer per la crittografia basata su file

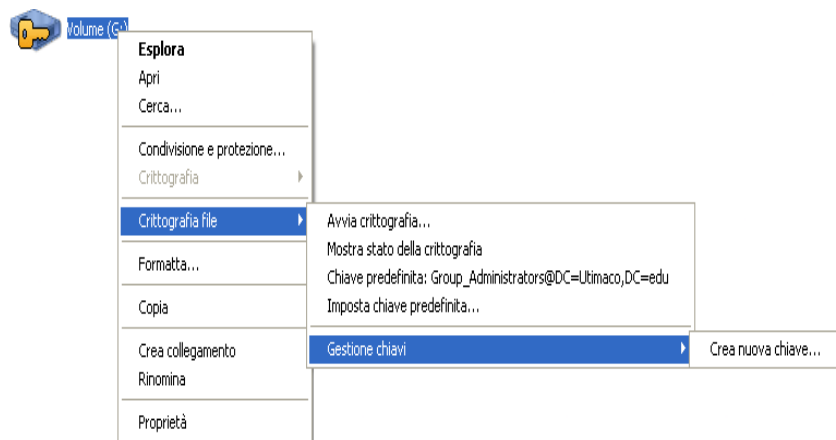
È possibile accedere alle funzioni per la crittografia basata su file tramite le rispettive voci dei menu di scelta rapida in Esplora risorse. Le funzioni sono disponibili nei menu di scelta rapida di

- volumi
- supporti rimovibili
- directory
- file

La voce **Crittografia file** è stata aggiunta al menu di scelta rapida. È possibile accedere alle singole funzioni tramite questo menu.

Se al volume selezionato non è stato applicato alcun criterio di crittografia basata su file, è possibile soltanto determinare lo stato della crittografia e visualizzare la finestra di dialogo per la generazione di nuove chiavi mediante il menu di scelta rapida.

Se al volume, al supporto rimovibile, alla directory o al file selezionato è stato applicato un criterio di crittografia basata su file, al menu di scelta rapida vengono aggiunte le seguenti voci:



Nota: Le funzioni visualizzate variano a seconda delle impostazioni definite nei criteri, e dipendono anche dal fatto se la funzione rilevante è disponibile o meno per il volume selezionato.

L'ambito delle funzioni varia in base al fatto se per il volume interessato è stata utilizzata la crittografia basata su file o basata su volume.

Sono disponibili le seguenti funzioni:

- **Avvia crittografia:** Se si sceglie questa opzione dal menu di scelta rapida di un volume, tutti i file possono essere crittografati o crittografati nuovamente.
- **Mostra stato della crittografia:** Indica se un volume, un supporto rimovibile o un file è stato crittografato; specifica la chiave utilizzata, se tale chiave è inclusa nel gruppo di chiavi dell'utente e se è possibile accedere a questo file.
- **Decrittografa:** Consente di decrittografare 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 crittografia basata su volume

Al menu di scelta rapida è stata aggiunta la voce **Crittografia**.

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

Nota: Crittografia file > Mostra stato della crittografia mostra lo stato della crittografia dei file sul volume dal punto di vista di una crittografia basata su file. I file presenti su un volume crittografato possono essere crittografati anche in modalità basata su file. In questo caso verrà visualizzata una finestra di dialogo corrispondente.

10.2.1 Aggiungi/rimuovi chiavi

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

È possibile assegnare chiavi al volume tramite la finestra di dialogo **Proprietà** del volume. Questa finestra di dialogo contiene la scheda Crittografia (fare clic con il pulsante destro del mouse su **Volume > Proprietà > Crittografia**).

Selezionare una chiave dall'elenco inferiore e fare clic 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 crittografato.

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

11 Crittografia dei dati

SafeGuard Enterprise crittografa i dati in un computer in due modalità: basata su volume o basata su file. Il responsabile della protezione definisce nei criteri di protezione i volumi (le unità) da crittografare.

11.1 Crittografia iniziale per la crittografia basata su file

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

Il simbolo della chiave gialla da solo non indica necessariamente che tutti i file presenti nell'unità siano già stati crittografati. Innanzitutto deve essere eseguita una crittografia iniziale.

Se è prevista la crittografia dei file, la crittografia iniziale viene avviata automaticamente oppure manualmente.

11.2 Crittografia trasparente

I file presenti su un'unità crittografata vengono crittografati in maniera trasparente. Non vengono visualizzati messaggi di avviso per la crittografia o la decrittografia quando l'utente apre, modifica e salva i file. Quando si apre un file, questo viene decrittografato ed è quindi possibile modificarlo. Al momento della chiusura o del salvataggio, il file viene nuovamente crittografato.

Se si copiano o si spostano file (anche mediante il comando Salva con nome) da un'unità crittografata a una posizione non crittografata nel computer, i file vengono decrittografati. I file vengono memorizzati nella nuova posizione in formato testo.

11.3 Restrizioni della crittografia iniziale dei computer protetti da SafeGuard Enterprise

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

Tuttavia, 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 non in linea, solo i criteri di crittografia 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 crittografia

Per tutti gli altri criteri che comportano l'attivazione della crittografia 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 venga 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 successivo all'installazione, mentre le chiavi definite dall'utente possono essere create nel computer soltanto dopo che questo sia stato registrato nel server SafeGuard Enterprise.

11.4 Crittografia basata su volume

Se il responsabile della protezione ha definito un criterio appropriato, la crittografia 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 sarà in grado di 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. Fare clic su **OK** per avviare la crittografia.

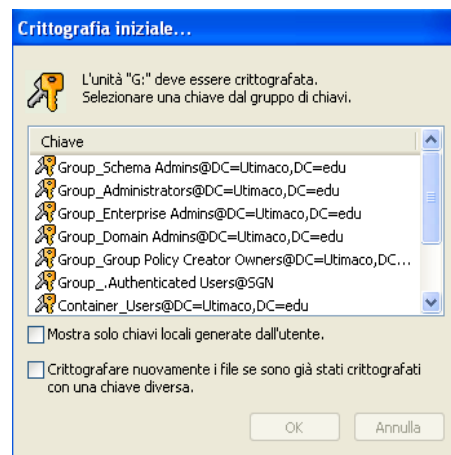
Durante il processo di crittografia, un Visualizzatore crittografia mostra lo stato di avanzamento della crittografia. Il visualizzatore è presente, ridotto a icona, sulla barra delle applicazioni di Windows e può essere aperto, semplicemente facendo clic sulla relativa icona. Se si desidera che il Visualizzatore crittografia rimanga ridotto a icona, è possibile richiedere la visualizzazione di una notifica quando la crittografia è stata completata, attivando l'opzione **Visualizza notifica prima della chiusura**. Il visualizzatore viene chiuso automaticamente al completamento della crittografia. Il volume crittografato può essere utilizzato normalmente come qualsiasi altro volume presente nel computer.

Nota: Per Windows 7 Professional, Enterprise e Ultimate, viene creata una partizione di sistema sui computer endpoint a cui non è stata assegnata una lettera di unità. Non è possibile crittografare la partizione di sistema mediante SafeGuard Enterprise.

11.5 Crittografia basata su file

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

1. Se la crittografia non viene attivata automaticamente, selezionare **Crittografia file > Avvia crittografia**.
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 sarà in grado di 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.

Nota: Per lo scambio di dati con altri utenti che dispongono di SafeGuard Enterprise installato nel computer, ma i quali non utilizzano la stessa chiave dell'utente che invia i dati, in genere sono richieste **chiavi locali generate dagli utenti**. Queste chiavi sono richieste inoltre per proteggere lo scambio di dati con utenti che non dispongono di SafeGuard Enterprise. È possibile identificare le chiavi locali in base al prefisso (Local_).

Nota: Se è attivata l'opzione **Crittografare nuovamente i file se sono già stati crittografati con una chiave diversa**, i file crittografati per i quali esiste una chiave verranno decrittografati e nuovamente crittografati utilizzando una nuova chiave.

3. Selezionare una chiave, quindi fare clic su **OK**.

Tutti i dati del volume interessato sono crittografati.

11.5.1 Definizione di una chiave predefinita

Definendo una chiave predefinita si specifica la chiave da utilizzare per la crittografia durante l'operazione.

1. È possibile definire la chiave predefinita tramite il menu di scelta rapida di un file presente su un volume o tramite il menu di scelta rapida del supporto rimovibile stesso.
2. Selezionare **Crittografia file > Imposta chiave predefinita** per aprire una finestra di dialogo o per selezionare la chiave.

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

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

11.5.2 Stato della crittografia

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

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

È possibile visualizzare lo stato della crittografia di un file tramite il rispettivo menu di scelta rapida. Selezionando **Crittografia file > Mostra stato della crittografia** è possibile aprire una finestra in cui è visualizzato lo stato della crittografia.

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

11.6 Restrizioni di accesso ai volumi

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

11.6.1 Volumi per cui la crittografia non è riuscita

Se è presente un criterio che definisce se un volume o tipo di volume debba essere crittografato e non è possibile eseguire il processo di crittografia, l'accesso a tale volume viene negato.

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

11.6.2 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 o come crittografati da SafeGuard Enterprise.

Se è presente un criterio che definisce che un volume di questo tipo deve essere crittografato, l'accesso a tale volume viene negato. Se si tenta di accedere al volume, viene visualizzato il relativo messaggio.

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

12 SafeGuard Data Exchange

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

Solo gli utenti che dispongono delle chiavi appropriate possono leggere il contenuto dei dati crittografati. Tutti i successivi processi di crittografia vengono eseguiti in modo trasparente. Crittografia trasparente significa che i dati che sono stati crittografati e salvati vengono automaticamente decrittografati da un'applicazione al momento del successivo accesso.

Una volta salvati, i file vengono nuovamente crittografati. Durante il lavoro quotidiano non si noterà che i dati vengono crittografati. Tuttavia, quando si scollega il supporto rimovibile, i dati resteranno crittografati e di conseguenza saranno protetti da accessi non autorizzati. 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, definire la crittografia come obbligatoria per i file memorizzati su tutti i supporti rimovibili. In questo caso tutti i file non crittografati esistenti sul dispositivo vengono inizialmente crittografati. Inoltre, tutti i nuovi file salvati su supporti rimovibili vengono crittografati. Se i file esistenti non devono essere crittografati, il responsabile della protezione può scegliere di consentire l'accesso ai file non crittografati esistenti. In questo caso SafeGuard Data Exchange non esegue la crittografia dei file esistenti non crittografati. Tuttavia i nuovi file vengono crittografati. Sarà dunque possibile leggere e modificare i file esistenti non crittografati, ma nel momento in cui uno di questi venga rinominato, verrà, di conseguenza, crittografato. In caso contrario non sarà consentito l'accesso ai file non crittografati e tali file non verranno crittografati.

Esistono due possibili metodi per scambiare file crittografati memorizzati su un supporto rimovibile:

- **SafeGuard Enterprise** è installato nel computer del destinatario dei file: 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 i dati al destinatario con la passphrase per la chiave.
- **SafeGuard Enterprise non** è installato nel computer del destinatario dei file: SafeGuard Enterprise fornisce SafeGuard Portable. Questa utilità può essere copiata automaticamente sul supporto rimovibile insieme ai file crittografati. Utilizzando SafeGuard Portable e la relativa passphrase, il destinatario può decrittografare i file e crittografarli nuovamente senza dover installare SafeGuard Data Exchange nel proprio computer.

12.1 Passphrase supporto singola per tutti i dispositivi rimovibili collegati al computer

SafeGuard Data Exchange consente di definire una sola passphrase del supporto per l'accesso a tutti i dispositivi rimovibili connessi al computer. Questa è indipendente dalla chiave utilizzata per la crittografia dei file.

Se specificato, l'accesso ai file crittografati può essere concesso presentando solo una passphrase del supporto. 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 di supporto ha senso negli scenari seguenti:

- Se si desidera utilizzare dati crittografati su supporti rimovibili anche su computer in cui SafeGuard Enterprise non è installato (SafeGuard Data Exchange in combinazione con SafeGuard Portable)
- Si desidera scambiare dati con utenti esterni: fornendo loro la passphrase del supporto, è possibile consentire loro l'accesso a tutti i file sul supporto rimovibile con un'unica passphrase indipendentemente dalla chiave utilizzata per la crittografia 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 crittografati con questa chiave. Tutti gli altri file non risulteranno leggibili.

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.

Nota: In questo caso, se specificato dal responsabile della protezione, l'accesso ai file crittografati su supporti rimovibili è completamente trasparente. Non è necessario presentare passphrase o password.

Nota: 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, verrà visualizzata una finestra di dialogo e in cui viene richiesto all'utente di immettere una passphrase del supporto o la passphrase di una chiave locale.

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):

- **Crittografia iniziale di tutti i file:** In questo caso la crittografia di tutti i dati presenti su un supporto rimovibile viene avviata non appena il dispositivo venga collegato al computer. Questa impostazione garantisce che i supporti rimovibili contengano esclusivamente dati crittografati. Quando si avvia la crittografia, viene chiesto di selezionare una chiave oppure viene utilizzata una chiave predefinita.
- **È consentito annullare la crittografia iniziale:** Quando viene avviata la crittografia iniziale, viene visualizzata una finestra di dialogo che consente di annullare la crittografia iniziale.
- **Non è consentito accedere ai dati non crittografati:** In questo caso SafeGuard Data Exchange accetterà solo dati crittografati sui supporti rimovibili. Se sui supporti rimovibili sono presenti dati non crittografati, il sistema non consentirà di accedervi. Sarà possibile accedere a questi dati solo dopo che i file sono stati crittografati.
- **È consentito decrittografare i file:** In questo caso è possibile decrittografare esplicitamente i file presenti sui supporti rimovibili. Un file che è stato decrittografato esplicitamente rimane in formato testo sul supporto rimovibile, se, ad esempio, viene trasferito a terze parti.
- **È possibile definire una passphrase di supporto per i supporti rimovibili:** La prima volta che si esegue la connessione a un supporto rimovibile, viene richiesto di immettere una passphrase del supporto.
- **Cartella di testo normale su supporto rimovibile:** Il responsabile della protezione può definire un cartella di testo normale che verrà creata su tutti i supporti rimovibili. I file di questa cartella non verranno crittografati da SafeGuard Data Exchange

12.1.1 Tipi di supporto supportati

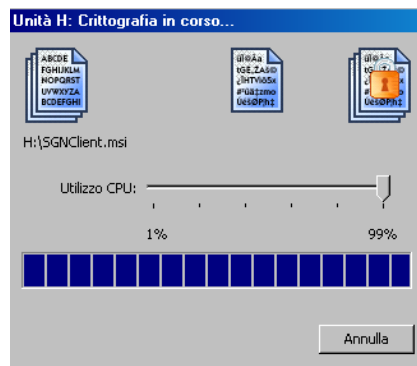
SafeGuard Data Exchange supporta i seguenti tipi di supporti rimovibili:

- Stick 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 (incl. ZIP, JAZ)

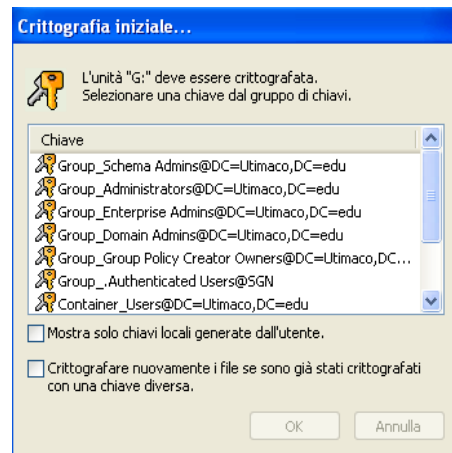
12.2 Crittografia di supporti rimovibili

12.2.1 Crittografia iniziale

La crittografia dei dati non crittografati presenti su supporti rimovibili ha inizio automaticamente al momento in cui i supporti vengono collegati al sistema oppure è necessario avviare il processo manualmente.



1. Per avviare il processo di crittografia, selezionare **Crittografia file > Avvia crittografia** dal menu di scelta rapida 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 fare clic su **OK**. Tutti i dati contenuti nei supporti rimovibili vengono crittografati.
3. 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 crittografia 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 richieste inoltre per proteggere 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 crittografati con una chiave esistente verranno decrittografati e nuovamente crittografati utilizzando la nuova chiave.

Timeout della crittografia iniziale

Se la crittografia iniziale è configurata per l'avvio automatico, è possibile avere il diritto di annullare la crittografia iniziale. In questo caso il pulsante **Annulla** è attivato, viene visualizzato un pulsante **Start** e l'avvio del processo di crittografia viene ritardato di 30 secondi. Se non si seleziona **Annulla** durante questo intervallo di tempo, la crittografia iniziale si avvia automaticamente dopo 30 secondi. Se si seleziona **Start**, la crittografia iniziale viene avviata immediatamente.

12.2.1.1 Crittografia iniziale in caso di utilizzo della passphrase di supporto

Se l'utilizzo di una passphrase di supporto è stato definito mediante un criterio, viene richiesto di immettere la passphrase di supporto prima della crittografia iniziale. La passphrase di supporto è valida per tutti i supporti rimovibili ed è associata al computer o a tutti i computer cui è possibile accedere.

La crittografia iniziale non verrà avviata prima di aver immesso la passphrase dei supporti. Dopo aver eseguito questa operazione, la crittografia iniziale si avvierà automaticamente.

Dopo aver immesso la passphrase dei supporti la prima volta, la crittografia iniziale si avvierà automaticamente durante la connessione di un dispositivo diverso al computer.

Nota: Nei computer in cui la passphrase dei supporti non è impostata, la crittografia iniziale non si avvierà.

12.2.2 Crittografia trasparente

Se le impostazioni definite per il computer specificano che i file sui supporti rimovibili debbano essere crittografati, tutti i processi di crittografia e decrittografia vengono eseguiti in modo trasparente.

I file vengono crittografati al momento in cui vengono scritti sui supporti rimovibili e decrittografati quando vengono copiati o spostati dai supporti rimovibili a una posizione diversa.

Nota: I dati vengono decrittografati soltanto se vengono copiati o spostati a una posizione alla quale non è applicato alcun criterio di crittografia. I dati sono quindi disponibili in questa posizione in formato testo. Se alla nuova posizione è applicato un criterio di crittografia diverso, i dati vengono crittografati in base a tale criterio.

12.2.2.1 Passphrase dei supporti

Se specificato dal criterio, viene chiesto di immettere la passphrase dei supporti quando si esegue per la prima volta la connessione a un dispositivo rimovibile dopo l'installazione di SafeGuard Data Exchange.

Se viene visualizzata la finestra di dialogo, leggere attentamente le informazioni in questa contenute e specificare la passphrase dei supporti. È possibile utilizzare questa passphrase dei supporti per accedere a tutti i file crittografati presenti nel supporto rimovibile, indipendentemente dalla chiave utilizzata per crittografarli.

La passphrase del supporto è valida per tutti i dispositivi connessi alla computer. Inoltre, la passphrase del supporto può essere utilizzata con SafeGuard Portable e consente l'accesso a tutti i file indipendentemente dalla chiave utilizzata per crittografarli.

12.2.2.2 Cambia/reimposta passphrase supporto

È possibile modificare la passphrase del supporto 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 è necessario immettere la passphrase precedente e quella nuova, quindi confermare quella nuova.

Se la passphrase del supporto è stata dimenticata, nella finestra di dialogo è disponibile l'opzione per reimpostarla. Se si attiva l'opzione **Reimposta passphrase supporto** e si seleziona **OK**, all'utente viene comunicato che la passphrase del supporto verrà reimpostata al prossimo accesso.

Disconnettersi immediatamente e rieseguire l'accesso. Selezionare quindi **Cambia passphrase supporto** dal menu dell'icona dell'area di notifica. All'utente viene comunicato che non sono presenti passphrase del supporto nel computer e sarà quindi necessario immetterne una nuova.

12.2.2.3 Sincronizzazione della passphrase dei supporti

La passphrase dei supporti presente nei dispositivi e nel computer verrà sincronizzata automaticamente. Se si cambia la passphrase del supporto nel computer e si connette il 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 cui si può accedere.

Nota: Dopo aver cambiato la passphrase del supporto, è necessario connettere tutti i supporti rimovibili con il computer. In questo modo, la nuova passphrase del supporto verrà immediatamente utilizzata in tutti i dispositivi (sincronizzazione).

12.2.2.4 Definizione di una chiave predefinita

Definendo una chiave predefinita si specifica la chiave da utilizzare per la crittografia durante l'operazione.

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. Inoltre, è possibile impostare immediatamente una chiave predefinita quando si crea la nuova chiave locale nella finestra di dialogo "Crea chiave".

Selezionare **Crittografia file > 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 crittografia successivi eseguiti sul supporto rimovibile. 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 crittografia. Se non è definita nel criterio, all'utente viene richiesto di specificare una chiave predefinita iniziale.

12.3 Scambio di dati utilizzando SafeGuard Data Exchange

Di seguito sono riportati alcuni esempi di scambio di dati protetto tramite SafeGuard Data Exchange:

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

In questo caso crittografare 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 crittografati.

- Scambio di dati con utenti SafeGuard Enterprise i quali non dispongono delle stesse chiavi dell'utente.

In questo caso creare una chiave locale e crittografare i dati utilizzando questa 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 la 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.

Inoltre, SafeGuard Portable deve essere copiato sul supporto rimovibile. È inoltre necessario fornire la passphrase al destinatario dei dati crittografati. Utilizzando la passphrase e SafeGuard Portable, il destinatario potrà decrittografare i file crittografati e, ad esempio, modificarli, quindi salvarli nuovamente in forma crittografata sul supporto rimovibile. Poiché SafeGuard Portable è un'applicazione autonoma, per poter accedere ai dati crittografati non è necessario installare alcun software aggiuntivo nel sistema host.

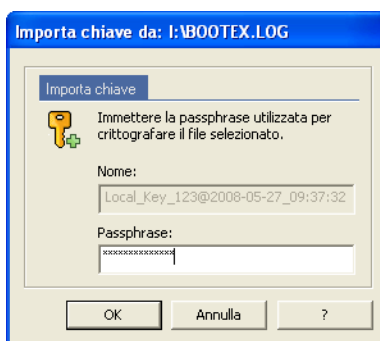
Nota: Il responsabile della protezione determina se SafeGuard Portable viene copiato nei supporti rimovibili mediante il criterio di protezione applicato all'utente.

12.3.1 Importazione di chiavi da un file

Se si ricevono supporti rimovibili contenenti dati che sono stati crittografati utilizzando chiavi locali definite dall'utente, è possibile importare nel proprio gruppo di chiavi la chiave necessaria per la crittografia.

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

Selezionare il file interessato nel dispositivo rimovibile quindi fare clic su **Crittografia file > Gestione chiavi > Importa chiave**.

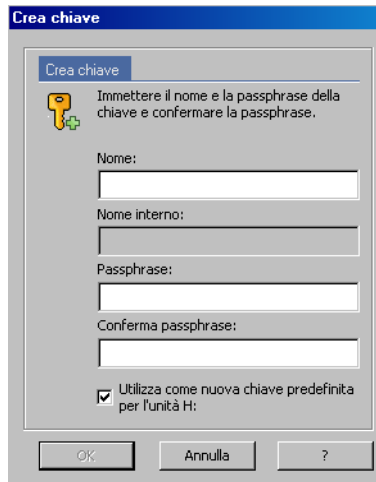


Immettere la passphrase nella finestra di dialogo visualizzata. La chiave viene importata ed è possibile accedere al file.

12.3.2 Creazione di chiavi locali per lo scambio di dati mediante SafeGuard

Per creare una chiave locale definita dall'utente, procedere come segue:

1. Fare clic sull'icona SafeGuard Enterprise dell'area di notifica nella barra delle applicazioni di Windows.
2. Fare clic su **Crea nuova chiave**.



3. Nella finestra di dialogo Crea chiave immettere un **Nome** e una **Passphrase** per la 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. Tuttavia si può anche decidere di utilizzare la passphrase semplice nonostante il messaggio di avviso. La passphrase deve rispettare i criteri aziendali definiti. In caso contrario, viene visualizzato un messaggio di avviso.

5. Mediante l'opzione **Usa 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 crittografia durante l'operazione e sarà valida fino a quando non ne verrà impostata un'altra.

6. Fare clic su **OK**.

La chiave viene creata e diviene disponibile a partire dal momento in cui i dati saranno stati sincronizzati con il server SafeGuard Enterprise.

Se si definisce questa chiave come predefinita, d'ora in poi tutti dati i copiati sul supporto rimovibile verranno crittografati utilizzando questa chiave.

Affinché il destinatario possa decrittografare tutti i dati presenti sul supporto rimovibile, potrebbe essere necessario crittografare nuovamente i dati sul supporto utilizzando la chiave creata localmente. A tale scopo, selezionare **Crittografia file > Avvia crittografia** dal menu di scelta rapida del dispositivo in Esplora risorse. Selezionare la chiave locale richiesta e crittografare i dati. Se si utilizza una passphrase di supporto, questa operazione non è necessaria.

12.4 Scrittura di file su CD e DVD mediante la Masterizzazione guidata CD di Windows

Nota: Con Windows XP, è possibile scrivere file su CD solamente utilizzando la Masterizzazione guidata CD di Windows. Windows XP non supporta la scrittura di file su DVD mediante la Masterizzazione guidata CD.

SafeGuard Data Exchange consente di scrivere file crittografati su CD mediante la Masterizzazione guidata CD di Windows.

Per eseguire questa operazione, è necessario specificare una regola di crittografia per l'unità di registrazione dei CD. SafeGuard Data Exchange aggiunge una finestra di dialogo alla Masterizzazione guidata CD. Nella finestra è possibile specificare la modalità di scrittura dei file sul CD (crittografati o formato testo).

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

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

In **Statistica** vengono visualizzate le informazioni seguenti:

- il numero dei file selezionati per essere scritti su CD
- il numero dei file crittografati
- il numero dei file in formato testo

In **Stato** sono visualizzate le chiavi utilizzate per la crittografia dei file già crittografati.

Per la crittografia dei file da scrivere sul CD viene sempre utilizzata la chiave specificata nella regola di crittografia per l'unità di registrazione dei CD.

È possibile che i file da scrivere sul CD risultino crittografati con chiavi diverse, se la regola di crittografia per l'unità di registrazione CD è stata modificata. Se la regola di crittografia è stata disattivata quando sono stati aggiunti i file, è possibile trovare i file in formato testo relativi nella cartella dei file da copiare sul CD.

12.4.1 Crittografia di file su CD

Per scrivere i file crittografati sul CD, fare clic su **Crittografa nuovamente tutti i file**.

Se necessario, i file già crittografati verranno crittografati nuovamente mentre i file in formato testo vengono crittografati per la prima volta. Sul CD i file vengono crittografati utilizzando la chiave specificata nella regola di crittografia per l'unità di registrazione CD.

12.4.2 Scrittura di file su CD in formato testo

Se si seleziona **Decrittografa tutti i file**, i file vengono prima decrittografati e poi scritti sul CD.

12.4.3 Copia di SafeGuard Portable sul supporto ottico

Se si seleziona questa opzione, anche SafeGuard Portable verrà copiato nel CD. Consente di leggere e modificare file crittografati con SafeGuard Data Exchange senza disporre di SafeGuard Data Exchange.

12.4.4 Masterizzazione di CD e DVD con Windows Vista

La Masterizzazione guidata CD di Windows Vista supporta la scrittura su CD e DVD.

La SafeGuard Disc Burning Extension per la Masterizzazione guidata CD è disponibile solo per la masterizzazione di CD e DVD in formato **Mastered**. La procedura guidata viene visualizzata solo se i file devono 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 crittografia per l'unità di registrazione, i file vengono crittografati automaticamente una volta copiati su CD/DVD.

12.5 SafeGuard Portable

Utilizzando SafeGuard Portable è possibile scambiare dati crittografati mediante supporti rimovibili con destinatari i quali non dispongono di SafeGuard Data Exchange installato nel computer. I dati crittografati con SafeGuard Data Exchange possono essere crittografati e decrittografati utilizzando SafeGuard Portable. L'operazione viene eseguita copiando automaticamente un programma (SGPortable.exe) sui supporti rimovibili.

Nota: SafeGuard Portable crittografa e decrittografa solo i file crittografati con AES 256.

L'utilizzo di SafeGuard Portable in combinazione con la relativa passphrase del supporto consente l'accesso a tutti i dati crittografati, indipendentemente dalla chiave utilizzata per crittografarli. In caso contrario la passphrase una chiave locale consente l'accesso unicamente ai file che sono stati crittografati mediante quella chiave specifica. Il destinatario può decrittografare i dati crittografati e crittografarli 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 tramite SafeGuard Data Exchange per la crittografia oppure creare una nuova chiave tramite SafeGuard Portable (ad esempio per nuovi file).

Non è necessario installare o copiare SafeGuard Portable nel computer del partner con il quale si stanno scambiando i dati. Il programma resta sul supporto rimovibile.

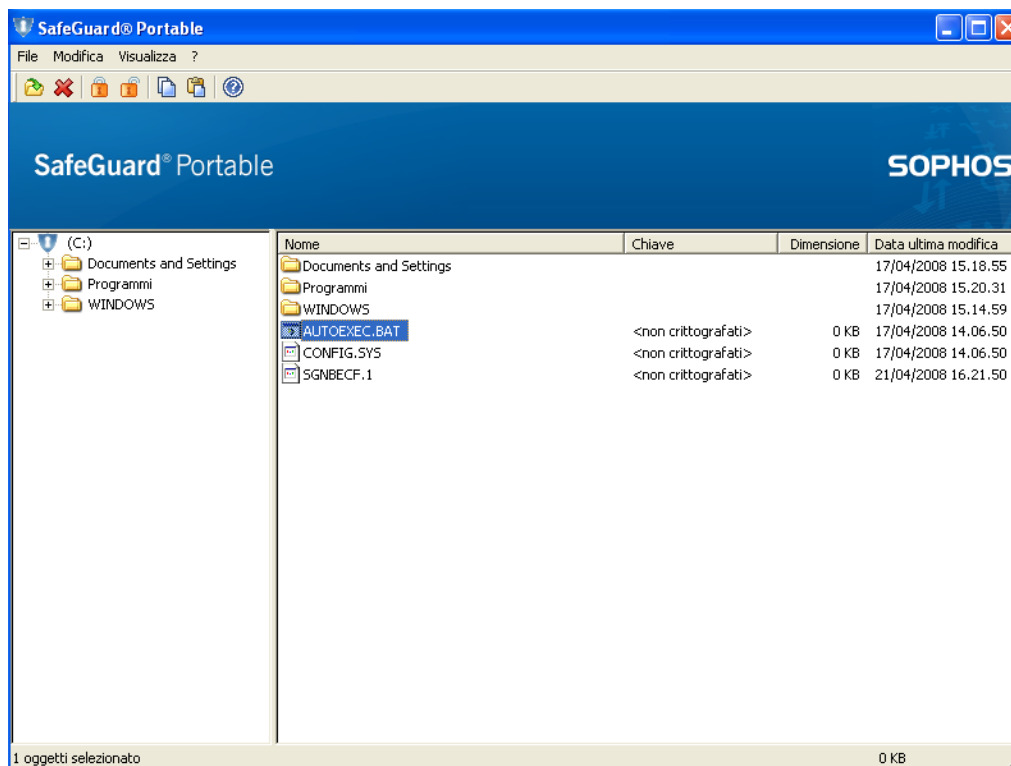
Nota: Se si è utenti di SafeGuard Enterprise, in genere non è necessario utilizzare SafeGuard Portable. La seguente descrizione riguarda gli utenti che non dispongono di SafeGuard Enterprise installato nel computer e che pertanto devono utilizzare SafeGuard Portable per modificare i dati crittografati.

12.5.1 Modifica di file utilizzando SafeGuard Portable

Si ricevono supporti rimovibili contenenti file crittografati con SafeGuard Data Exchange accompagnati da una cartella denominata `SGPortable`. Questa cartella contiene il file `SGPortable.exe`.

1. Avviare SafeGuard Portable facendo doppio clic su `SGPortable.exe`.

Utilizzando SafeGuard Portable è possibile decrittografare i dati crittografati presenti sui supporti rimovibili e crittografarli nuovamente. SafeGuard Portable fornisce funzionalità simili a quelle offerte in Esplora risorse di Windows.



Oltre ai dettagli dei file già noti visualizzati in Esplora risorse (nome, dimensioni, ecc), in SafeGuard Portable è riportata anche la colonna **Chiave**. Questa colonna indica se i dati sono crittografati o meno. Se un file è crittografato, nella colonna è visualizzata la chiave utilizzata.

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

2. Per modificare i file presenti sul supporto rimovibile, selezionare i file facendo clic su di essi con il pulsante sinistro del mouse e scegliere il comando appropriato dal menu di scelta rapida (facendo clic con il pulsante destro del mouse) oppure dal menu **File**.

I seguenti comandi sono disponibili dal menu di scelta rapida:

| | |
|---------------------------------------|---|
| Imposta chiave di crittografia | Aprire la finestra di dialogo Immettere la chiave . In questa finestra è possibile generare una chiave di crittografia tramite SafeGuard Portable. |
| Crittografa | Consente di crittografare il file selezionato sul supporto rimovibile. Per la crittografia viene scelta l'ultima chiave utilizzata. |
| Decrittografa | Aprire la finestra di dialogo Inserire la passphrase . Immettere la passphrase per la decrittografia del file selezionato in questa finestra di dialogo. |
| Stato della crittografia | Consente di visualizzare una finestra di dialogo che mostra lo stato della crittografia del file. |
| Copia in | Consente di copiare il file in una cartella di propria scelta e di decrittografarlo. |
| Elimina | Consente di eliminare il file selezionato sul supporto rimovibile. |

È possibile anche selezionare i comandi **Apri**, **Elimina**, **Crittografa**, **Decrittografa** e **Copia** utilizzando le icone presenti nella barra delle applicazioni.

12.5.1.1 Impostazione di chiavi di crittografia

Per crittografare un file presente nel supporto rimovibile e creare una chiave di crittografia:

1. Dal menu di scelta rapida o dal menu **File**, selezionare **Imposta chiave di crittografia**.
Viene visualizzata la finestra di dialogo **Immettere la chiave**.
2. Immettere un **Nome** e una **Passphrase** per la chiave. **Confermare** la passphrase e fare clic su **OK**.
La passphrase deve rispettare i criteri aziendali definiti. In caso contrario, viene visualizzato un messaggio di avviso.

La chiave verrà creata e verrà utilizzata d'ora in poi per la crittografia.

12.5.1.2 Crittografia

Per crittografare un file presente nel supporto rimovibile:

1. In SafeGuard Portable Explorer, selezionare il file e, mediante il menu di scelta rapida, fare clic su **Crittografa**.

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

Quando si salvano nuovi file sul supporto rimovibile utilizzando la procedura di trascinamento selezione, viene richiesto se si desidera crittografarli.

In questo caso, se non è stata eseguita alcuna crittografia con SafeGuard Portable in precedenza, verrà visualizzata una finestra di dialogo per l'impostazione della chiave. Immettere nella finestra di dialogo il nome della chiave e la passphrase (la quale deve essere confermata). Fare clic su **OK**.

2. Selezionare il file da crittografare con la chiave appena impostata e fare clic su **Crittografa** dal menu di scelta rapida oppure dal menu **File**.

Il file viene crittografato e, completato il processo, viene visualizzato un apposito messaggio.

Nota: L'ultima chiave utilizzata e impostata da SafeGuard Portable verrà utilizzata per tutti i processi di crittografia successivi eseguiti con SafeGuard Portable, a meno che non venga impostata una chiave diversa.

12.5.1.3 Decrittografia

Per decrittografare un file presente nel supporto rimovibile:

1. Selezionare il file in SafeGuard Portable Explorer, quindi fare clic su **Decrittografa** 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 fare clic su **OK**.

Il file è stato decrittografato.

La passphrase del supporto consente di accedere a tutti i file crittografati sul supporto rimovibile, indipendentemente dalla chiave utilizzata per crittografarli. Se si dispone solo della passphrase di una chiave locale, sarà possibile accedere solo ai file che sono stati crittografati con questa chiave.

Quando si decrittografa un file che è stato crittografato utilizzando una chiave generata in SafeGuard Portable, tale file viene decrittografato automaticamente.

Dopo aver decrittografato i file sul supporto rimovibile e immesso la passphrase della chiave, la prossima volta che si crittografano o si decrittografano file crittografati con la stessa chiave, non sarà necessario immettere nuovamente la passphrase.

SafeGuard Portable memorizza la passphrase per tutto il tempo in cui l'applicazione viene eseguita. Per la crittografia viene scelta l'ultima chiave utilizzata da SafeGuard.

Dopo la decrittografia, i file sono disponibili in formato testo sul supporto rimovibile. I file decrittografati vengono crittografati automaticamente alla chiusura di SafeGuard Portable.

12.5.1.4 Crittografia di nuovi file utilizzando SafeGuard Portable

Inoltre, è possibile copiare i propri file su supporti rimovibili in forma già crittografata utilizzando SafeGuard Portable.

A tale scopo:

1. È sufficiente spostare i file richiesti su SafeGuard Portable Explorer mediante il trascinamento della selezione.
Verrà chiesto se si desidera crittografare il file interessato.
2. Confermare di aver crittografato il file con l'ultima chiave utilizzata e di averlo copiato sul supporto rimovibile.

12.5.1.5 Stato della crittografia

Per determinare lo stato della crittografia di un file:

1. Selezionare il file e fare clic su **Stato della crittografia** dal menu di scelta rapida o dal menu **File**.
Lo stato della crittografia verrà inoltre indicato nella colonna **Chiave** accanto al nome del file in SafeGuard Portable Explorer.

12.5.2 Altre operazioni eseguibili mediante SafeGuard Portable

Sono inoltre disponibili le seguenti operazioni:

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

Quando si apre un file crittografato tramite questo comando, viene chiesto di immettere la passphrase. Immettere la passphrase e fare clic su **OK**. Il file viene crittografato e aperto.

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

- **Copia in:** Questo comando è disponibile solo nel menu di scelta rapida, accessibile mediante il pulsante 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

Utilizzando SafeGuard Configuration Protection è possibile definire le interfacce e i dispositivi periferici consentiti sui computer degli utenti. Questo impedisce l'introduzione di 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.

In generale, le porte o i dispositivi del computer possono essere abilitati o bloccati utilizzando criteri appropriati. Inoltre, l'utilizzo da parte di determinati dispositivi può essere limitato.

È possibile impostare restrizioni per determinati dispositivi per le porte:

- USB
- PCMCIA
- Firewire

Per queste porte è possibile definire con esattezza 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 in generale, viene visualizzato un messaggio di notifica una volta ricevuto il criterio contenente questa informazione. La porta non potrà essere utilizzata.

Il messaggio di notifica viene visualizzato come descrizione comando dell'icona di protezione separata 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.

14 SafeGuard Enterprise e BitLocker

La crittografia di unità BitLocker è una funzionalità completa di crittografia 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 crittografia per il volume di avvio.

14.1 Criteri di crittografia per BitLocker

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

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

14.2 Crittografia iniziale nel computer protetto da BitLocker

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

Quando SafeGuard Enterprise viene installato nel PC, l'icona del prodotto SafeGuard Enterprise viene visualizzata nell'area di notifica della barra delle applicazioni del PC. 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 degli utenti.



Nota: Se un disco rigido crittografato 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.

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

14.3 Decrittografia con BitLocker

I computer degli utenti crittografati con BitLocker non possono essere decrittografati automaticamente. La decrittografia 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 o una combinazione di entrambi.

Il responsabile della protezione può impostare varie modalità di accesso in un criterio in SafeGuard Management Center e distribuire il criterio ai PC BitLocker.

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

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

14.4.1 Trusted Platform Module (TPM)

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

14.4.2 Stick USB

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

14.4.3 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 Lenovo Rescue and Recovery

Per informazioni sulle versioni di Lenovo Rescue and Recovery (RnR) supportate da SafeGuard Enterprise, vedere l'articolo della Knowledge Base disponibile all'indirizzo seguente:
<http://www.sophos.com/support/knowledgebase/article/108383.html>.

È possibile ripristinare i backup completi dei sistemi operativi su una partizione crittografata senza dover prima decrittografare il disco rigido. Ciò consente di risparmiare molto tempo durante l'esecuzione di un ripristino di emergenza. Le funzionalità di SafeGuard Enterprise sono state ufficialmente certificate da Lenovo.

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 riavviato, 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 che non dispongono di supporto amministrativo. In un viaggio di lavoro, risulta utile, ad esempio, per ripristinare il computer.

15.1 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 il back up efficace e il metodo di recupero insieme alle partizioni crittografate del sistema operativo SafeGuard Enterprise. I backup di sistemi SafeGuard Enterprise crittografati 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 crittografia rimangono inalterate, non è necessario reinstallare alcun software. Non è necessario riavviare la crittografia.

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

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

15.2 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 vedere la Knowledge Base: <http://www.sophos.com/support/knowledgebase/article/108383.html>
- Lenovo Rescue and Recovery può essere utilizzato per recuperare i volumi SafeGuard Enterprise crittografati. È necessario installare il pacchetto di installazione `SGNClient.msi`.
- Per Rescue and Recovery i volumi devono essere crittografati con la chiave del computer definita. Per i volumi crittografati con altre chiavi, Rescue and Recovery non è supportato.

15.3 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 nella partizione virtuale "C:" (partizione principale del disco rigido master) sul disco rigido del computer.

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

15.3.1 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 possano essere ripristinati backup non autorizzati.

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

15.3.2 SafeGuard Enterprise Device Encryption è già installato

I passaggi necessari per l'installazione di Rescue and Recovery dipendono dalla posizione di RnR WinPE.

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

In questo caso non viene eseguita alcuna impostazione di SafeGuard Enterprise per l'ambiente RnR WinPE. L'utente deve avviare uno strumento di SafeGuard Enterprise denominato `SetupWinPE.exe` per impostare RnR WinPE per l'utilizzo integrato con SafeGuard Enterprise. Questo strumento esegue tutte le modifiche necessarie per l'ambiente WinPE.

Nota: `SetupWinPE.exe` può essere utilizzato anche se l'installazione corrente di RnR viene aggiornata a una nuova versione. In caso di aggiornamento di RnR, si consiglia di avviare nuovamente `SetupWinPE.exe` per accertarsi che vengano eseguite tutte le modifiche WinPE necessarie.

Nota: Questo strumento locale può essere utilizzato solo per un RnR WinPE presente su un disco rigido locale.

- a) Installare Rescue and Recovery nel disco rigido locale.
- b) Avviare lo strumento seguente:
`SetupWinPE.exe -r`
- c) Riavviare il sistema operativo Windows.

- RnR WinPE si trova su un CD-ROM o su un disco rigido esterno

Quando WinPE viene creato dalla funzione RnR Create Rescue and Recovery Media tutte le modifiche necessarie sono già state eseguite per l'ambiente RnR WinPE.

- a) Installare Rescue and Recovery.
- b) Riavviare il sistema operativo Windows.

15.3.3 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 necessarie 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).

15.4 Aggiornamento

L'aggiornamento implica che SafeGuard Enterprise e Rescue and Recovery siano installati e che si desideri aggiornare uno o entrambi alla nuova versione.

15.4.1 Aggiornamento di SafeGuard Enterprise

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

15.4.2 Aggiornamento di Rescue and Recovery

Se si aggiorna Rescue and Recovery, eseguire SetupWinPE.exe prima di riavviare il sistema dopo l'aggiornamento.

15.5 Disinstallazione

Quando si disinstallano prodotti 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 SafeGuard Enterprise è ancora installato, le modifiche di RnR del settore di avvio di MBR vengono rimosse e viene ripristinato il settore di avvio di MBR originale.

15.6 Ambiente di avvio e opzioni di recupero

SafeGuard Enterprise consente l'avvio nell'ambiente Rescue and Recovery dopo aver eseguito l'accesso all'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 crittografati 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 l'Autenticazione all'accensione e non saranno disponibili chiavi, pertanto non sarà possibile accedere ai volumi crittografati. Se Rescue and Recovery viene avviato direttamente da BIOS, il sistema operativo verrà recuperato. Durante il processo di ripristino SafeGuard Enterprise verrà rimosso. Per proteggere nuovamente il sistema, è necessario reinstallare SafeGuard Enterprise.

15.7 Creazione di un backup

I backup vengono creati in Windows mediante Rescue and Recovery. Su computer in cui Rescue and Recovery è già installato, e SafeGuard Enterprise verrà installato successivamente, viene visualizzato un messaggio che avvisa l'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 in:

- disco rigido locale
- secondo disco rigido
- disco rigido USB
- rete
- memory stick USB
- CD/DVD

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

15.8 Ripristino di backup dei file

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

15.9 Ripristino del sistema SafeGuard Enterprise

Per ripristinare un backup di sistema che include SafeGuard Enterprise, eseguire l'avvio nell'ambiente Rescue and Recovery. L'ambiente RnR viene visualizzato non appena si preme uno dei tasti seguenti 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) Immettere le credenziali per SafeGuard Enterprise.

2. Se non si utilizza un computer Lenovo:

- a) Accedere all'Autenticazione all'accensione con le proprie credenziali di SafeGuard Enterprise.
- b) Durante la fase di avvio del computer, premere **F11** per avviare l'ambiente Rescue and Recovery.

Viene visualizzata l'interfaccia utente di Rescue and Recovery. Viene visualizzata la schermata iniziale.

3. Fare clic 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.

15.10 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: Queste partizioni sono disponibili sul computer e non verranno crittografate neanche se è stato definito un criterio di crittografia, ad esempio, per la crittografia di tutti i volumi.

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

15.11 Autenticazione all'accensione disabilitata e Lenovo Rescue and Recovery

Nel caso in cui Autenticazione all'accensione non sia attiva per il 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, vedere la documentazione di Lenovo Rescue and Recovery.

16 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.com/support/>
- Scaricando la documentazione del prodotto su <http://www.sophos.com/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.

17 Copyright

Copyright © 1996 - 2010 Sophos Group e Utimaco Safeware AG. Tutti i diritti riservati.

Nessuna parte di questa pubblicazione può essere riprodotta, memorizzata in un sistema di recupero informazioni, o trasmessa, in qualsiasi forma o con qualsiasi mezzo, elettronico o meccanico, inclusi le fotocopie, la registrazione 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.

Sophose è un marchio registrato di Sophos Plc e Sophos Group. SafeGuard è un marchio registrato di Utimaco Safeware AG - a member of the Sophos Group. Tutti gli altri nomi di società e prodotti qui menzionati sono marchi o marchi registrati dei rispettivi titolari.

Tutti i prodotti SafeGuard sono diritti d'autore di Utimaco Safeware AG - a member of the Sophos Group, o, come applicabili, i suoi concessionari di licenza. Tutti gli altri prodotti Sophos sono diritti d'autore di Sophos plc., o, come applicabili, i suoi concessionari di licenza.

Le informazioni di copyright di venditori parte terza sono disponibili nel file Disclaimer and Copyright for 3rd Party Software.rtf presente sulla directory del prodotto.