

Sophos SafeGuard Disk Encryption, Sophos SafeGuard Easy Guida alla versione demo

Versione prodotto: 5.60

Data documento: aprile 2011



Sommario

- 1 Introduzione.....3
- 2 Requisiti.....4
- 3 Pacchetto di configurazione demo5
- 4 Installazione del software demo.....5
- 5 Cosa aspettarsi dopo l'installazione del software.....5
- 6 Cosa aspettarsi dalla versione completa.....14
- 7 Esecuzione dell'upgrade alla versione completa.....17
- 8 Disinstallazione del software demo.....19
- 9 Supporto tecnico.....19
- 10 Note legali.....19

1 Introduzione

Questo documento accompagna nell'esecuzione della versione demo di client SafeGuard Disk Encryption. La versione demo consente di testare il processo completo di cifratura del disco di SafeGuard, comprendente le operazioni di installazione e l'esecuzione di Power-on Authentication (POA, autenticazione durante la fase di preavvio).

Questa versione demo funge da client demo comune per i seguenti prodotti che eseguono lo stesso motore client di SafeGuard:

■ Sophos SafeGuard Disk Encryption (SDE)

Soluzione di cifratura del disco completa per hard drive locali. È inclusa nella licenza di Sophos Endpoint Security and Data Protection (ESDP). La configurazione dei criteri di cifratura viene eseguita tramite SafeGuard Policy Editor. Per distribuire tali criteri ai computer endpoint, è necessario possedere una versione con licenza di SafeGuard Policy Editor.

Per ulteriori informazioni, consultare la pagina web <http://www.sophos.it/products/enterprise/endpoint/security-and-control/>.

■ SafeGuard Easy (SGE)

Simile a SDE, fornisce supporto anche per l'autenticazione tramite impronte digitali di Lenovo, i token non di cifratura e gli hard drive esterni, oltre che supportare ambienti di runtime aventi due installazioni Windows cifrate in parallelo nello stesso computer. La configurazione dei criteri di cifratura viene eseguita tramite SafeGuard Policy Editor. Per distribuire tali criteri ai computer endpoint, è necessario possedere una versione con licenza di SafeGuard Policy Editor.

Per ulteriori informazioni, consultare la pagina web <http://www.sophos.it/products/enterprise/encryption/safeguard-easy/>.

Per eseguire la valutazione del client SafeGuard Disk Encryption, viene fornito un pacchetto di configurazione in versione demo avente le impostazioni dei criteri già preconfigurate, [consultare la sezione Pacchetto di configurazione in versione demo](#) a pagina 5. Tali impostazioni dei criteri non possono essere modificate nella versione demo. Il pacchetto di configurazione in versione demo deve essere distribuito su computer di prova con installazione client SDE/SGE 5.60, [consultare la sezione Installazione del software demo](#) a pagina 5.

Il pacchetto di configurazione in versione demo SGNDemoClientConfig.msi è reperibile nella cartella di installazione di consegna prodotto di Sophos SafeGuard Disk Encryption/SafeGuard Easy. Il pacchetto di configurazione in versione demo è disponibile per il download alla pagina web <https://secure.sophos.it/products/enterprise/free-trials/safeguard-easy/>.

Se interessati a una protezione che vada oltre la cifratura del disco locale, **SafeGuard Enterprise** è il prodotto che fa al caso proprio. SafeGuard Enterprise è il prodotto di cifratura ammiraglio di Sophos, completo di gestione centralizzata integrata online di Active Directory, reportistica, autenticazione multifattoriale (tramite impronte digitali di Lenovo, smartcard o token crypto) e gestione delle chiavi avanzata per per la cifratura di supporti rimovibili e il controllo delle porte. Per SafeGuard Enterprise è disponibile una versione demo a parte comprendente SafeGuard Management Center e tutti i relativi moduli. Per ricevere questa versione demo contattare un responsabile alle vendite di Sophos. Per ulteriori informazioni, consultare la pagina web <http://www.sophos.it/products/enterprise/encryption/safeguard-enterprise/>.

Una volta portata a termine la valutazione è possibile passare alla versione completa della soluzione di cifratura fornita da SafeGuard. È possibile eseguire l'upgrade del client demo a Sophos SafeGuard Disk Encryption, SafeGuard Easy o SafeGuard Enterprise. Per una breve panoramica su cosa aspettarsi dalle versioni con licenza, [consultare la sezione Cosa aspettarsi dalla versione completa](#) a pagina 14.

2 Requisiti

Per eseguire l'installazione del pacchetto di configurazione SGNDemoClientConfig.msi di SafeGuard Disk Encryption Demo in un computer di prova, sono necessari i seguenti prerequisiti:

- Il client Sophos SafeGuard Disk Encryption (SDE)/SafeGuard Easy (SGE) con Device Encryption deve essere installato.
- Il client SDE/SGE non deve essere stato configurato utilizzando un pacchetto di configurazione regolare creato tramite una versione con licenza di SafeGuard Policy Editor.

Per eseguire l'installazione del client SDE/SGE tramite Device Encryption, sono necessari i seguenti requisiti di sistema:

- Windows XP SP2 o successivo (32 bit)
- Windows Vista SP1 (a 32 bit)
- Windows Vista SP1 (a 64 bit)
- Windows 7 (a 32 o 64 bit)
- Minimo 1 GB di RAM
- Minimo 1 GB di spazio disco libero
- Unità IDE o SATA (no SCSI). Per informazioni sulla compatibilità dell'hardware, consultare l'articolo in inglese <http://www.sophos.com/support/knowledgebase/article/107781.html>.
- Se si sta eseguendo Lenovo Rescue and Recovery, assicurarsi di essere in possesso della versione 4.21 o successiva.

Nel caso di dubbi sulle piattaforme supportate, installare il software. Il programma di installazione riporterà tutti gli eventuali problemi rilevati e l'operazione verrà annullata.

Nota:

il programma di installazione a 64 bit richiede un download a parte da sophos.com.

Prima di installare il software assicurarsi di essere in possesso dei diritti amministrativi per il computer client in cui si desidera installarlo.

Nota:

questo software viene distribuito al solo scopo di valutazione e non può essere eseguito nei computer aziendali. Per eseguire l'upgrade dalla versione demo a quella completa, è necessario possedere licenze valide. Per ulteriori informazioni, [consultare la sezione Recupero con Local Self Help](#) a pagina 17.

3 Pacchetto di configurazione demo

Per eseguire la valutazione del client SafeGuard Disk Encryption, viene fornito un pacchetto di configurazione in versione demo avente le impostazioni dei criteri già preconfigurate. Questo pacchetto di configurazione deve essere distribuito su computer di prova con installazione client SDE/SGE 5.60, [consultare la sezione Installazione del software demo](#) a pagina 5.

Il pacchetto di configurazione in versione demo SGNDemoClientConfig.msi è reperibile nella cartella di installazione di consegna prodotto di Sophos SafeGuard Disk Encryption/SafeGuard Easy. Il pacchetto di configurazione in versione demo è disponibile per il download alla pagina web <https://secure.sophos.it/products/enterprise/free-trials/safeguard-easy/>.

Il pacchetto di configurazione in versione demo comprende la seguente configurazione client:

- Tutte le unità interne sono cifrate.
- Tutti gli utenti con diritti di amministratore Windows possono disinstallare il software.
- La procedura di recupero del Local Self Help per il ripristino dell'accesso, nel caso di password dimenticate, risulta abilitata e preconfigurata.
- L'accesso tramite smartcard/token è disabilitato.
- Tutti gli utenti possono importare ulteriori utenti SafeGuard e consentire loro di accedere tramite autenticazione all'accensione.

Nota:

queste impostazioni preconfigurate non possono essere modificate nella versione demo.

4 Installazione del software demo

1. Installare il client Sophos SafeGuard Disk Encryption/SafeGuard Easy e Device Encryption nel computer di prova. Per ulteriori informazioni, consultare la guida all'avvio di Sophos SafeGuard Disk Encryption/SafeGuard Easy.
2. Installare il pacchetto di configurazione demo SGNDemoClientConfig.msi nel computer di prova.

Se si cerca di installare il pacchetto di configurazione demo senza avere prima installato il client Sophos SafeGuard Disk Encryption/SafeGuard Easy, viene visualizzato un messaggio di errore. Lo stesso vale nel caso in cui il client sia già stato configurato utilizzando un pacchetto di configurazione regolare creato tramite SafeGuard Policy Editor con licenza.

3. Riavviare e testare il computer.

5 Cosa aspettarsi dopo l'installazione del software

Una volta riavviato il computer di prova, la prima schermata che viene visualizzata è quella relativa alle note legali. Si tratta di una funzione del criterio opzionale che è possibile abilitare durante la distribuzione di SafeGuard Disk Encryption nel proprio ambiente. Nella versione completa del prodotto, il testo è interamente personalizzabile. In questo caso, leggere le note legali e cliccare su **OK**.



5.1 Windows XP

5.1.1 Password Windows già impostata

1. Viene visualizzata la schermata di accesso a Windows.
2. Inserire le proprie credenziali Windows e accedere a Windows.

A questo punto, SafeGuard Disk Encryption sincronizza le credenziali Windows con il suo sistema di Power-on Authentication (POA).

Nota:

SafeGuard Disk Encryption utilizza le credenziali Windows per la Power-on Authentication.

Si consiglia quindi di attivare Local Self Help, in modo tale da poter disporre di un dispositivo di recupero nel caso in cui le credenziali vengano dimenticate, [consultare la sezione Attivazione di Local Self Help](#) a pagina 9.

5.1.2 Password Windows non impostata

Se non si è configurata alcuna password Windows, verrà ora richiesto di farlo.

1. Viene visualizzato un messaggio di **Password non valida**, seguito dalla finestra di dialogo **Modifica** per la definizione della password.
2. Dal momento che non si è in possesso di alcuna password, lasciare vuoto il campo **Password precedente**.
3. Nel campo **Nuova password**, digitare una parola o frase che si possa ricordare. Digitrala di nuovo nel campo **Conferma**.

È necessario ricordare la password per poter accedere all'unità cifrata e avviare il computer.

Si consiglia quindi di attivare Local Self Help, in modo tale da poter disporre di un dispositivo di recupero nel caso in cui le credenziali vengano dimenticate, [consultare la sezione Attivazione di Local Self Help](#) a pagina 9.

5.2 Windows Vista e Windows 7

Windows Vista e Windows 7 eseguono una procedura di autenticazione diversa rispetto a Windows XP. Se in possesso di uno di questi sistemi operativi, si può verificare quanto riportato di seguito.

5.2.1 Password Windows già impostata

1. Una volta eseguito il caricamento del sistema operativo, come di solito si apre immediatamente il desktop, con l'unica differenza che questa volta viene visualizzata la finestra di dialogo riportata qui di seguito:



2. Inserire la password.

Viene eseguito il caricamento del desktop e SafeGuard Disk Encryption effettua la sincronizzazione delle credenziali. Al prossimo avvio del computer sarà possibile accedere alla Power-on Authentication utilizzando queste credenziali.

Se non viene visualizzata l'icona a forma di buco della serratura, prima di eseguire l'accesso selezionate **Cambia utente** e poi tale icona.

Si consiglia quindi di attivare Local Self Help, in modo tale da poter disporre di un dispositivo di recupero nel caso in cui le credenziali vengano dimenticate, [consultare la sezione Attivazione di Local Self Help](#) a pagina 9.

5.2.2 Password Windows non impostata

Dopo avere cliccato su **OK** nella finestra di dialogo relativa alle note legali, Windows viene caricato e si accede, come di solito, direttamente al desktop. Per come è configurata la versione demo, le credenziali Windows devono essere sincronizzate tramite Power-on Authentication.

Nota:

SafeGuard Disk Encryption utilizza le credenziali Windows per la Power-on Authentication.

1. Per eseguire la sincronizzazione, viene visualizzata la finestra di dialogo **Accesso a Sophos SafeGuard**.

2. Dal momento che non si è in possesso di alcuna password, cliccare semplicemente su **OK**. Viene visualizzato un messaggio relativo alla **Modifica password di Sophos SafeGuard**.

Ciò è dovuto al fatto che SafeGuard Disk Encryption non accetta password con un numero di caratteri pari a zero.

3. Cliccare su **OK**.

Viene ora richiesto di modificare la password. Viene visualizzata la finestra di dialogo **Modifica** per la scelta della password.

Dal momento che non si è in possesso di alcuna password, lasciare vuoto il campo **Password precedente**.

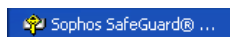
4. Nel campo **Nuova password**, digitare una parola o frase che si possa ricordare. Digitala di nuovo nel campo **Conferma**.

È necessario ricordare la password per poter accedere all'unità cifrata e avviare il computer.

Si consiglia quindi di attivare Local Self Help, in modo tale da poter disporre di un dispositivo di recupero nel caso in cui le credenziali vengano dimenticate, [consultare la sezione Attivazione di Local Self Help](#) a pagina 9.

5.3 Procedura di cifratura dell'hard drive

Una volta eseguito l'accesso a Windows, nella barra delle applicazioni viene visualizzata una scheda:



Cliccare su questa scheda per visualizzare il livello di progresso della cifratura iniziale.

Nota:

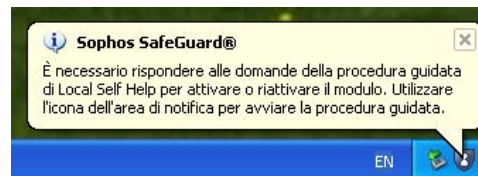
durante la cifratura iniziale, è possibile riscontrare un rallentamento delle prestazioni del sistema.



È quindi possibile continuare a lavorare o arrestare il computer. Se si sceglie di arrestare il computer, la procedura di cifratura iniziale continua.

5.4 Attivazione di Local Self Help

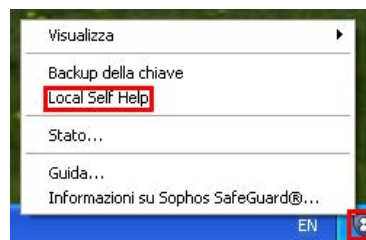
Una volta eseguito l'accesso al proprio desktop, viene visualizzato il seguente messaggio:



Si tratta di un messaggio informativo sulla possibilità di attivare il Local Self Help. Local Self Help consente il recupero delle credenziali dimenticate rispondendo a una serie di domande la cui risposta è stata fornita durante l'attivazione del Local Self Help.

Per attivare Local Self Help:

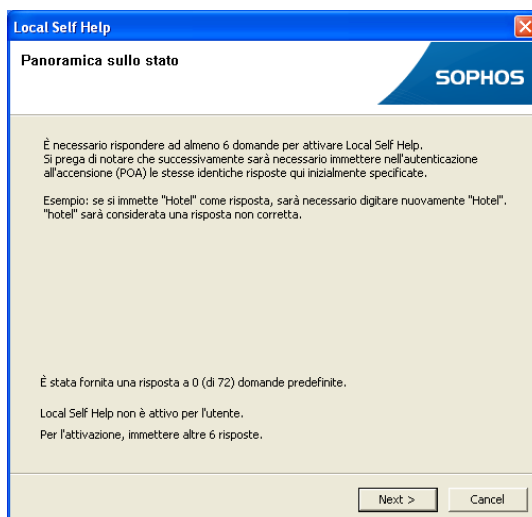
1. Cliccare col tasto destro del mouse sull'icona a forma di scudo nella barra delle applicazioni e cliccare su **Local Self Help**.



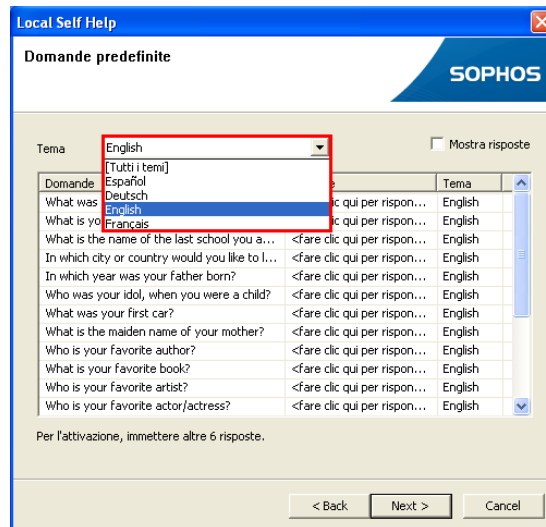
2. Viene richiesto di inserire nuovamente le proprie credenziali:



3. Inserire il nome utente e la password Windows, quindi cliccare su **Avanti**.



4. Questa pagina fornisce uno stato. Cliccare su **Avanti**.



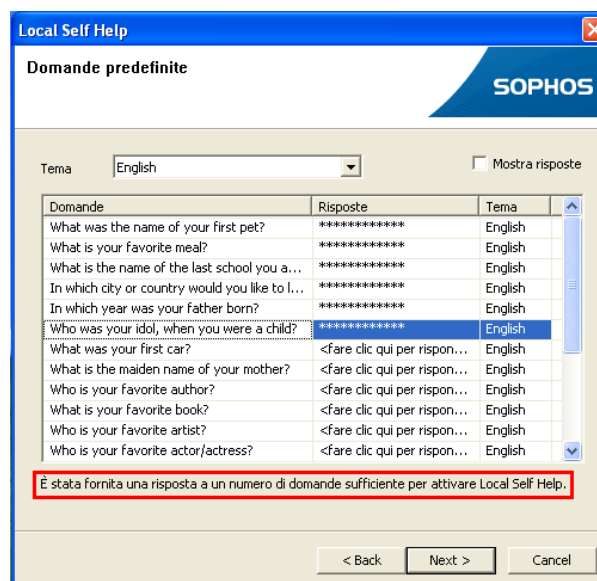
5. Nella finestra di dialogo **Domande predefinite**, dall'elenco a discesa **Tema** selezionare una lingua. È ora possibile iniziare a rispondere alle domande.

Tenere presente che le risposte fanno distinzione fra maiuscole o minuscole.

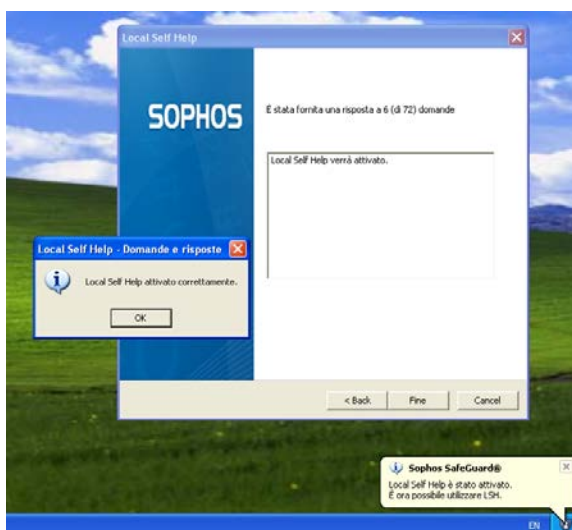
Nota:

Per il giapponese, sotto Windows XP è necessario installare il supporto linguistico adeguato. In caso contrario, le domande in giapponese potrebbero essere visualizzate in modo non corretto.

Una volta risposto a sei domande lo stato visualizzato nella parte bassa della finestra di dialogo cambia.



6. Cliccare su **Avanti** e poi su **Fine**.



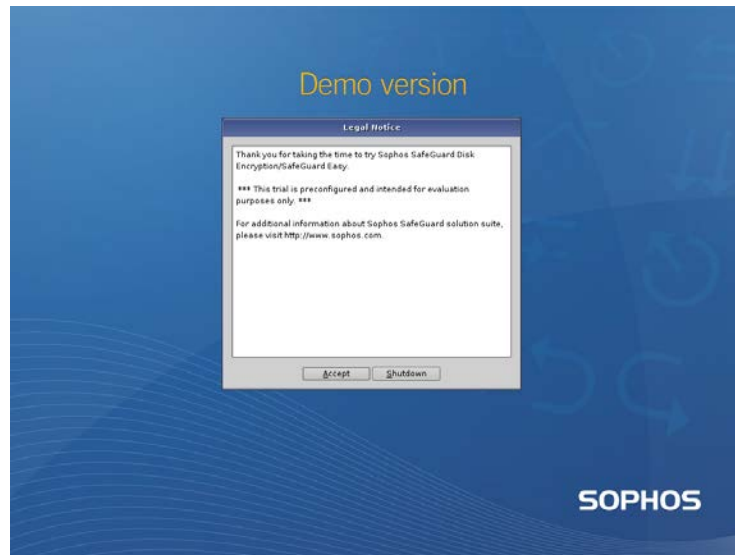
Local Self Help è ora attivo.

5.5 Riavvio successivo

Al riavvio successivo del computer viene abilitata la Power-on Authentication. La prima schermata visualizzata è quella relativa alle note legali.

1. Per procedere cliccare su **Accetto**.

Nella versione completa del prodotto, sia la finestra di dialogo relativa alle note legali che quella riportata qui di seguito sono personalizzabili per poter ridurre al minimo l'impatto visivo sugli utenti finali. Nella versione demo invece l'impatto visivo è forte e le finestre non sono configurabili.



2. Una volta superata la finestra relativa alle note legali, è possibile accedere alla Power-on Authentication. Immettere le credenziali nei campi relativi e cliccare su **OK**.



SafeGuard Disk Encryption convalida le credenziali e consente il caricamento di Windows. Finché non vengono inserite credenziali valide, nessuno potrà accedere ai dati contenuti nell'unità.

A questo punto, la configurazione del software è completata. Tutte le specifiche funzioni disponibili nella versione completa dipendono da quale versione del prodotto si è acquistata (Sophos SafeGuard Disk Encryption (ESDP bundle)/SafeGuard Easy o SafeGuard Enterprise). Informazioni dettagliate sono reperibili nel sito web di Sophos.

5.6 Recupero della password con Local Self Help

Nel caso si sia dimenticata la password utilizzata per accedere a Windows durante la configurazione di SafeGuard Disk Encryption, è possibile recuperarla tramite il Local Self Help. Se sono stati eseguiti i passaggi descritti in questa guida, Local Self Help sarà attivo e pronto ad eseguire il recupero dell'accesso, [consultare la sezione Attivazione di Local Self Help](#) a pagina 9.

Per ripristinare il proprio sistema nel caso di password dimenticata:

1. Inserire il nome utente e cliccare su **Recupero**.



2. Viene visualizzata la finestra di dialogo Benvenuti a Local Self Help. Questa finestra fornisce una breve descrizione dei passaggi che seguiranno. Cliccare su **Avanti**.
3. Verrà ora richiesto di rispondere a tre delle sei domande a cui si è data risposta durante la configurazione. Le risposte fanno distinzione fra maiuscole e minuscole. Per poter continuare è necessario rispondere a tutte e tre le domande in modo corretto. Una risposta errata viene considerata da SafeGuard come un tentativo di accesso non riuscito. Per motivi di sicurezza il sistema non indica quale delle risposte date è risultata errata.
4. Solo dopo avere risposto a tutte le domande correttamente, è possibile cliccare sulla finestra blu per recuperare la password dimenticata, o semplicemente su **OK** per poter accedere a Windows.

6 Cosa aspettarsi dalla versione completa

Le seguenti sezioni forniscono una panoramica sulle funzionalità e i benefici delle versioni complete di Sophos SafeGuard Disk Encryption, SafeGuard Easy e SafeGuard Enterprise.

Utilizzare il sito web sophos.com o contattare il proprio responsabile alle vendite, se si desidera ricevere maggiori informazioni sulla gamma di prodotti SafeGuard o ordinare una versione con licenza completa.

6.1 Benefici della versione completa con licenza

La versione demo rappresenta solo uno spaccato sulle potenzialità della cifratura del disco completa fornite dalla gamma dei prodotti SafeGuard.

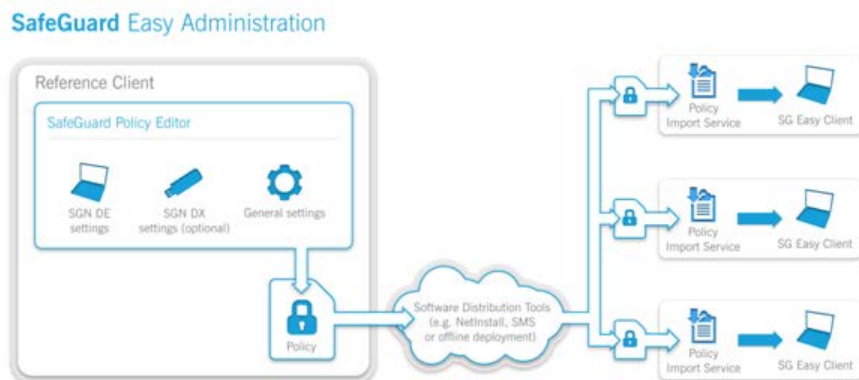
L'esecuzione dell'upgrade alla versione completa consente di:

- Avere controllo totale sui criteri di cifratura, compresa la cifratura di dispositivi aggiuntivi e la configurazione di bitmap di sfondo, oltre che la creazione di messaggi di notifica all'utente.
- Utilizzare metodi di recupero aggiuntivi nel caso di password dimenticate (Challenge/Response) e fornire supporto nel ripristinare installazioni di sistemi operativi interrotte, anche in unità cifrate, tramite l'immagine di ripristino avviabile di Virtual Client basata su Windows PE.
- Utilizzare, se lo si desidera, dischi rigidi autocifranti conformi a Opal e gestiti da SafeGuard, completi di tutte le opzioni di preavvio e gestione offerte dalle soluzioni software di SafeGuard.
- Aggiungere smartcard, token e/o opzioni di autenticazione biometrica (SafeGuard Easy o SafeGuard Enterprise).
- Aggiungere la gestione online, comprendente sincronizzazione di Active Directory, gestione API, accesso centralizzato, reportistica e gestione delle chiavi (SafeGuard Enterprise).
- Aggiungere, quando si sceglie di eseguire l'upgrade a SafeGuard Enterprise, moduli funzionali aggiuntivi per la cifratura di supporti rimovibili, compreso supporti ottici (SafeGuard Data Exchange), controllo dispositivi e porte (SafeGuard Configuration Protection) o gestione BitLocker (SafeGuard PartnerConnect).
- Ricevere aggiornamenti e supporto per i prodotti ovunque ci si trovi da Sophos e dai partner Sophos.

6.2 Varianti di gestione fra cui scegliere

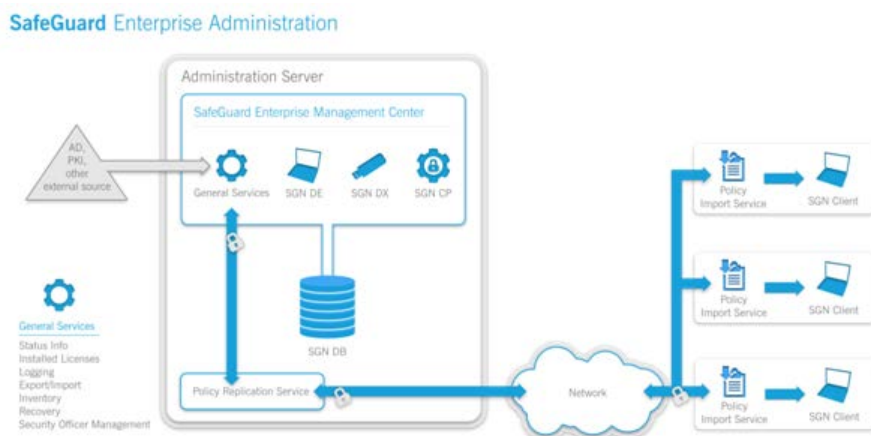
SafeGuard Easy (SGE) e Sophos SafeGuard Disk Encryption (SDE) vengono gestiti in modalità autonoma; i criteri sono quindi creati in un client di riferimento e distribuiti tramite una procedura di distribuzione prodotta da terzi. Eseguendo questa versione demo è possibile valutare un client SGE/SDE. L'esecuzione dell'upgrade alla versione completa richiede l'installazione di SafeGuard Policy Editor e l'importazione di una licenza valida. È quindi possibile creare un pacchetto di configurazione con licenza e distribuirlo ai client demo.

Il diagramma riportato qui di seguito mostra il funzionamento della modalità di gestione di SafeGuard Easy/Sophos SafeGuard Disk Encryption:



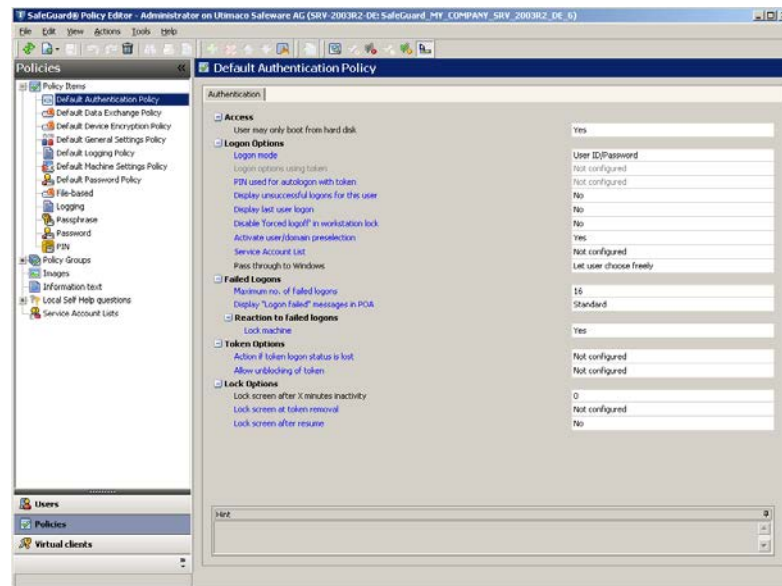
SafeGuard Enterprise viene gestito online tramite un servizio web che autorizza anche l'importazione di Active Directory, l'accesso centralizzato e la reportistica relativa allo stato, oltre che ulteriori moduli di sicurezza quali SafeGuard Data Exchange per la cifratura di dispositivi rimovibili basata su gruppi e SafeGuard Configuration Protection per il controllo di porte e dispositivi. Per eseguire l'upgrade dalla versione demo è necessario installare il server di gestione di SGN e il SafeGuard Management Center, oltre che distribuire un pacchetto di configurazione con licenza ai client demo. In questo modo i client demo diventano client gestiti che si connettono a SGN Server.

Il diagramma riportato qui di seguito mostra il funzionamento della gestione online di SafeGuard Enterprise. In un contesto in cui si esegue SGN gestito, un sottoinsieme di client può essere gestito anche in modalità offline, vale a dire in una modalità identica a quella descritta nel diagramma precedente relativo a SafeGuard Easy.



6.3 Esempi di schermate delle varianti di gestione

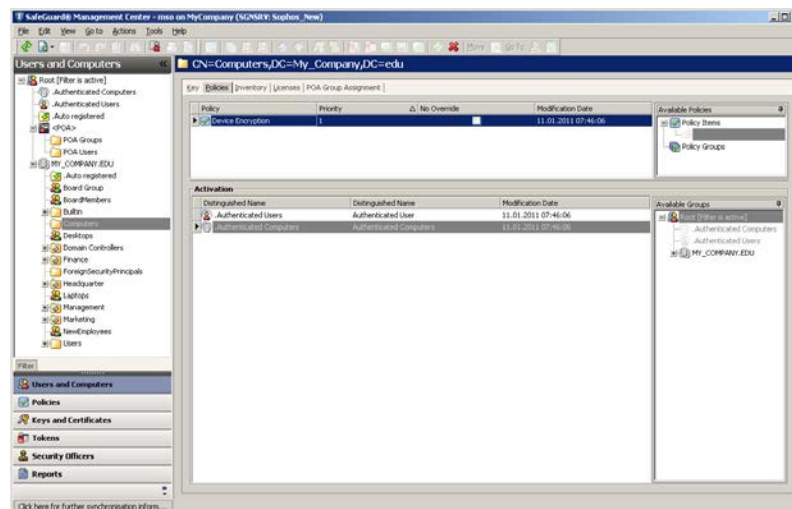
L'immagine riportata qui di seguito mostra SafeGuard Policy Editor per SafeGuard Easy. SafeGuard Policy Editor per Sophos SafeGuard Disk Encryption (SDE) è sostanzialmente uguale. Ha semplicemente opzioni dei criteri meno avanzate, per esempio non contempla criteri per Data Exchange e per l'accesso tramite impronte digitali.



Nota:

gli elementi dell'interfaccia di Active Directory, gestione del Security Officer, report, chiavi, certificati ecc. non sono necessari e quindi non presenti nella modalità autonoma (SGE/SDE); lo sono, al contrario, in SafeGuard Enterprise Management Center.

L'immagine riportata qui di seguito mostra la gestione **Utenti e Computer** in the SafeGuard Management Center.



7 Esecuzione dell'upgrade alla versione completa

Una volta portata a termine la valutazione è possibile passare alla versione completa della soluzione di cifratura fornita da SafeGuard.

È possibile eseguire l'upgrade del client demo a:

- Sophos SafeGuard Disk Encryption/SafeGuard Easy, [consultare la sezione Esecuzione dell'upgrade a Sophos SafeGuard client](#) a pagina 18.
- SafeGuard Enterprise, [consultare la sezione Esecuzione dell'upgrade a Sophos SafeGuard client](#) a pagina 18.

Per poter eseguire l'upgrade è necessario possedere licenze valide. Per poterle ottenere, si prega di contattare il responsabile alle vendite più vicino.

Per eseguire l'upgrade, creare un nuovo pacchetto di configurazione contenente i relativi tool di gestione con licenza e distribuirlo ai computer.

Nota:

non è necessario rimuovere la versione demo.

Nota:

non è possibile eseguire l'upgrade di un client demo a una versione completa più recente. Per prima cosa è necessario eseguire l'upgrade del client demo al client con licenza della stessa versione, quindi aggiornarlo alla versione più recente.

7.1 Esecuzione dell'upgrade a un client Sophos SafeGuard

1. Assicurarsi di avere a disposizione SafeGuard Policy Editor con licenza.

Per informazioni dettagliate su come installare e configurare SafeGuard Policy Editor con licenza, consultare la guida all'avvio di Sophos SafeGuard Disk Encryption/SafeGuard Easy.

2. In SafeGuard Policy Editor, creare un nuovo pacchetto di configurazione.

Per informazioni dettagliate, consultare la guida all'avvio di Sophos SafeGuard Disk Encryption/SafeGuard Easy.

3. Distribuire il pacchetto di configurazione appena creato al computer di prova.

Una volta eseguito l'upgrade a una versione completa, viene avviata la procedura di backup automatico della chiave. Gli utenti importati durante il processo di valutazione del software non vengono rimossi e continueranno a poter accedere al computer. Per ulteriori informazioni, consultare la guida in linea di Sophos SafeGuard Disk Encryption/SafeGuard Easy Administrator e la guida in linea per utenti.

7.2 Esecuzione dell'upgrade a un client SafeGuard Enterprise

1. Assicurarsi di avere a disposizione SafeGuard Management Center con licenza.

Per informazioni dettagliate su come installare e configurare SafeGuard Enterprise e SafeGuard Management Center con licenza, consultare il manuale di installazione di SafeGuard Enterprise.

2. In SafeGuard Management Center, creare un nuovo pacchetto di configurazione.

Per informazioni dettagliate, consultare il manuale di installazione di SafeGuard Enterprise.

3. Distribuire il pacchetto di configurazione appena creato al computer di prova.

Una volta eseguito l'upgrade a una versione completa, viene avviata la procedura di backup automatico della chiave. La Power-on Authentication riporta all'accesso automatico e il primo utente Windows che accede al computer ne diventa il proprietario. Per ulteriori informazioni, consultare la guida in linea di SafeGuard Enterprise Administrator e la guida in linea per utenti.

8 Disinstallazione del software demo

Nel caso si decida di non eseguire l'upgrade della configurazione client a una versione completa, è possibile rimuovere il software demo dal computer di prova eseguendo la procedura riportata qui di seguito.

Nota:

quando si eseguire l'upgrade a una versione completa, non è necessario disinstallare il software demo, *consultare la sezione Esecuzione dell'upgrade alla versione completa* a pagina 17. Utilizzare il sito web sophos.com o contattare il proprio responsabile alle vendite, se si desidera ricevere maggiori informazioni sulla gamma di prodotti SafeGuard o ordinare una versione con licenza completa.

1. Aprire **Aggiungi/rimuovi programmi**.
2. Rimuovere "Sophos SafeGuard 5.60 Client Configuration" e "Sophos SafeGuard 5.60 Client".

Quando si esegue la rimozione del client, comincerà la decifratura dell'unità. Si consiglia di disinstallare entrambi i pacchetti per consentire la decifratura completa dell'unità prima del riavvio.

Se durante questa procedura il sistema viene riavviato, l'operazione di disinstallazione viene cancellata, mentre quella di decifratura continuerà al riavvio del sistema. Una volta portata a termine la decifratura, è possibile dare nuovamente inizio alla rimozione del client di cifratura di SafeGuard.

9 Supporto tecnico

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

- Visitando il forum SophosTalk su <http://community.sophos.com/> e cercando altri utenti con lo stesso problema
- Visitando la knowledge base del supporto Sophos su <http://www.sophos.it/support/>
- Scaricando la documentazione del prodotto su <http://www.sophos.it/support/docs/>
- Inviando un'e-mail a support@sophos.com, indicando il o i numeri di versione del software Sophos in vostro possesso, i sistemi operativi e relativi livelli di patch, ed il testo di ogni messaggio di errore.

10 Note legali

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

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

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

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